

Public Document Pack



SELKIRK COMMON GOOD FUND SUB COMMITTEE WEDNESDAY, 15TH FEBRUARY, 2023

The following item of additional business will be considered at the MEETING of the SELKIRK COMMON GOOD FUND SUB COMMITTEE to be held VIA MICROSOFT TEAMS on WEDNESDAY, 15 FEBRUARY 2023 at 3.00 pm.

All Attendees, including members of the public, should note that the public business in this meeting will be livestreamed and video recorded and that recording will be available thereafter for public view for 180 days.

J. J. WILKINSON,
Clerk to the Council,

14 February 2023

ADDITIONAL BUSINESS			
8	(a)	Application for Financial Assistance Consider application for financial assistance from Selkirk Means Business (Selkirk BID) (Copy attached.)	(Pages 3 - 182) 20 mins

NOTES

- 1. Timings given above are only indicative and not intended to inhibit Members' discussions.**
- 2. Members are reminded that, if they have a pecuniary or non-pecuniary interest in any item of business coming before the meeting, that interest should be declared prior to commencement of discussion on that item. Such declaration will be recorded in the Minute of the meeting.**

Membership of Committee:- Councillors C. Cochrane (Chair), L. Douglas, E. Thornton-Nicol and Community Councillor I. King

Please direct any enquiries to Declan Hall 01835 826556
Email:-- Declan.Hall@scotborders.gov.uk

This page is intentionally left blank

Common Good Fund: Application Form for 2022/23*

*Please note this is a fund of last resort – you will need to demonstrate to the Common Good Fund Committee that you have tried to secure funding from other sources.

Applicant Group/Organisation:	Selkirk Means Business Ltd (Selkirk BID)
Name of your project:	Replacement and extension of CCTV provision in Selkirk Town Centre
The name of the Common Good Fund that you are applying to:	Selkirk Common Good

What does your organization do and who does it support? If appropriate. (max. 100 words)

Tell us what your group does, the activities it undertakes and in what way it benefits the community.

Selkirk Means Business Limited is a Business Improvement District (BID); a not-for-profit company created to manage and deliver the projects and services within the BID area. Selkirk Means Business Limited is dedicated to improving and making Selkirk town centre a better place to work and to conduct business.

Selkirk Means Business has a mission to encourage sustainable economic growth to Selkirk Town Centre. By pooling resources and working in partnership with existing organizations and bodies, Selkirk Means Business will work to lift Selkirk and drive economic regeneration.

Summarise what you want to use this funding for (max. 100 words)

(i.e. will it increase access, improve quality of life etc.)

The existing CCTV system in the centre of Selkirk is no longer fit for purpose, the overall system has been obsolete for some time and currently none of the existing cameras are functioning.

Selkirk Means Business's original Business Plan included the refreshing of the CCTV system under the objective "Helping Businesses to Thrive". Having received ongoing assurance and support from both businesses and the local community that CCTV was a positive addition to the town, we agreed to deliver this objective by not only replacing the existing CCTV system but by expanding the coverage by adding three new points that will mean the town centre's hot spots are covered, in addition the system has been designed to allow future expansion and alterations if required.

Summarise how the outcomes of the project will be measured/evaluated (max. 100 words)

It is anticipated that anti-social behaviour in the public spaces will reduce dramatically and vandalism to the street furniture, bus shelters and signs stopped.

All requests for access to the CCTV will be documented, and support any future evaluation of the CCTV's success and usefulness. This will include the ability to assess any outlying areas potentially not covered by the system and pin point any potential areas that may benefit from future expansion.

Tell us how your activity/project will make a difference to your organisation and how it will benefit the residents of the current/former Burgh (max. 200 words)

Tell us what activities you plan to carry out and how you will deliver it.

When considering the refurbishment of the CCTV system in January 2020 we carried out a short Facebook poll to gather feedback. The post reached 2,788 members of the wider community and generated 401 engagements. The response was clear: 95% of votes said that the CCTV needed updating. Only 5% saying they did not like the CCTV plan.

Recently, the Selkirk community came together for two community meetings – bringing 190 residents and business owners to discuss Selkirk's future. Initial feedback from each meeting highlighted that security was valued and regarded it as a positive attribute about living in Selkirk. They said:

"We want a town that is clean, with more local amenities, more bins, no litter, no plastic and no vandalism. And less anti-social behaviour."

The impact on businesses to avoid damage to property or have the ability to check footage if damage does occur is clear. The cameras will be a deterrent for disorderly behaviour in public places; they will discourage vandalism; litter dropping and encourage dog walkers to pick up mess.

CCTV will provide security and peace of mind for families, older members of community as well as businesses.

Tell us how your project will be sustainable in the future (max. 100 words)

Write here ...

The CCTV equipment is guaranteed for one year, which is standard for this type of equipment, but the overall life expectancy of the full system is considerably longer and it is anticipated, at the very minimum, will last at least ten years. The ongoing maintenance and the cost of the scheme which will be covered by local sponsorship and income generated from the proposed admin processing fee of £20 for requests to access footage from the system.

The system is fully futureproofed, as it is a wireless system, both software + hardware updates can be updated if required in the future + as previously highlighted, the system has been designed to allow expansion and variations ensuring the town continues to benefit from a high specification CCTV system long term and not become obsolete as the current system.

The system is able to be fully accessible by Police officers, giving real time footage remotely by mobile signal, at any time, this allows the officers to both assess and react swiftly to any potential disturbance locally or area wide as well as use the footage for any potential prosecutions.

Expenditure: Please tell us how much money you need for the entire activity/project (you may be asked to provide up to 3 quotes to support your application)

Item of Expenditure	Cost (£)
Radio infrastructure	£10,700 (ex VAT)
CCTV & NVR	£18,900 (ex VAT)
Total Expenditure	£29,600 (ex VAT)
How much would you like from the Common Good Fund?	£9,995
Please supply a copy of your signed & dated Annual Accounts or Projected Financial Plan	Attached

Have you received funding in the last 5 years from Scottish Borders Council or any other external funders? If so, please detail the fund name, the amount and the purpose of the grant.		
Fund	Amount	Purpose
SBC	£5K	Year one funding - contributing to development of website, street furniture and contribution to cycle station costs.
Selkirk Common Good Fund	£4.5K	Development of cycle station and cycle friendly location in the High Street
SBC and Scottish Government	£21K	Shop Front Scheme – supporting tidying up of 21 businesses in the centre of town.
SOSEP	£20K	Feasibility Study into Car Parking expansion and Haining collaborations.
SBC – COVID Funding	£8K	To support the provision of PPE equipment for businesses, supporting the promotion of “Selkirk, Open for Business” to encourage “shopping local”.
Scottish Town Partnership	£2.5K	To support the provision of PPE equipment for businesses, supporting the promotion of “Selkirk, Open for Business” to encourage “shopping local”.
Scottish Town Partnership	£3K	Town Trade Tradition. Showcasing the town’s manufacturing heritage, working with the General Store to promote and provide retail space in the centre of town.
Scotland Loves Local Grant	£4,650	Improvements and refurbishment of Halliwell’s Close, working in collaboration with Live Borders.
Scotland Loves Local Grant	£2,750	Improvements to Selkirk’s Market Place to encourage the return of events.
SBC – Place Based Investment Plan	£20K	To improve the town centre’s closes, due to be complete summer 2023 (in a similar way to Halliwell’s Close improvements).

Tell us about your own fundraising or how you have secured other funding for this project.

	Amount	Purpose
Money collected through the BID levy	£22,525	Providing security and piece of mind to businesses in BID area.
Private sponsorship	£3,000	To provide specific coverage for the War Memorial.

Individual/Group/Organisation details:

Contact Name:	David Anderson
Position in Group/Org: (if appropriate)	Chair
Home Address:	██████████ ██████
Post Code:	██████
Telephone Number:	██████████
Email Address:	████████████████████
Date:	
Signature:	

Equalities

Do you have an Equal Opportunities Policy or Equality Statement? Yes No

Explain how your project complies with the obligations contained in the Equality Act 2010

CCTV signage will be positioned in public space areas where CCTV cameras are located and in operation. The signage is required to be placed in these areas under the Data Protection Act (DPA) and in accordance to the CCTV Codes of Practice to allow persons the opportunity to modify their behaviour prior to entering a camera zone in which any identified illegal or anti-social behaviour will be reported to relevant law enforcement partners for action and/or such activity which may have been captured and recorded and used later by partners for investigation and possible prosecution.

The signage will also provide details of the CCTV owner and contact details.

Public Protection

Does your idea/project involve work with children, young people under the age of 18 or vulnerable adults? Yes No

If yes what public protection policies do you have in place and how often are these reviewed? Please provide a copy of these or give full details below.

Write here...

NA

Permissions

Does your project involve work to a building or land? Yes No

If yes do you have the following? (please tick relevant)

- A lease agreement (Date of lease _____ and duration _____ years)
- Written permission of owner
- Planning permission (Reference No. 22/00994/FUL)

Common Good Funds

Common Good Funds in Scotland originated in the 15th century and are the assets and income of some of the current/former Burghs. They can represent a substantial portfolio of land, property, some moveable items and investments and by law continue to exist for the benefit of the inhabitants of the former Burghs to which they relate. Scottish Borders Council is the owner of these Funds and each Fund has a sub-committee comprising the relevant local Councillors who make the decisions on the management of the Fund's assets and approval of any requests for funding (up to a limit of £20,000 above which full Council approval is required).

If you are successful in being awarded Common Good Funds, you will be asked to complete a monitoring & evaluation form when your project is complete or within 1 year of receiving funding. Future applications will not be considered until this has been received and the Common Good Fund Sub-Committee are satisfied with the evaluation you have provided.

This completed form and supporting documents should be submitted to Democratic Services, Scottish Borders Council, Council Headquarters, Newtown St Boswells, TD6 0SA. Email: compap@scotborders.gov.uk Telephone: 01835 825005

This page is intentionally left blank

Company registration number: SC591540

Selkirk Means Business Ltd
Unaudited financial statements
31 March 2022

Selkirk Means Business Ltd

Contents

	Page
Directors and other information	1
Directors report	2
Statement of financial position	3 - 4
Statement of changes in equity	5
Notes to the financial statements	6 - 7

Selkirk Means Business Ltd

Directors and other information (continued)

Directors Stuart Davidson
 David Anderson
 Tracey Ward
 Caroline Cochrane

Company number SC591540

Registered office 15 High Street
 Selkirk
 TD7 4BZ

Selkirk Means Business Ltd

**Directors report (continued)
Year ended 31 March 2022**

The directors present their report and the unaudited financial statements of the company for the year ended 31 March 2022.

Directors

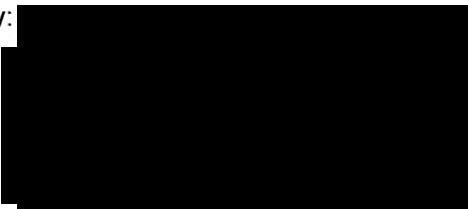
The directors who served the company during the year were as follows:

Stuart Davidson
David Anderson
Tracey Ward
Caroline Cochrane

Small company provisions

This report has been prepared in accordance with the provisions applicable to companies entitled to the small companies exemption.

This report was approved by the board of directors on 20 December 2022 and signed on behalf of the board by:



David Anderson
Director

Selkirk Means Business Ltd

**Statement of financial position
31 March 2022**

	Note	2022 £	£	2021 £	£
Fixed assets					
Tangible assets	6	108		218	
			108		218
Current assets					
Debtors	7	4,100		10,328	
Cash at bank and in hand		14,969		17,702	
		19,069		28,030	
Creditors: amounts falling due within one year	8	(19,069)		(28,030)	
Total assets less current liabilities			108		218
Net assets			108		218
Capital and reserves					
Profit and loss account			108		218
Shareholders funds			108		218

For the year ending 31 March 2022 the company was entitled to exemption from audit under section 477 of the Companies Act 2006 relating to small companies.

Directors responsibilities:

- The members have not required the company to obtain an audit of its financial statements for the year in question in accordance with section 476;
- The directors acknowledge their responsibilities for complying with the requirements of the Act with respect to accounting records and the preparation of financial statements.

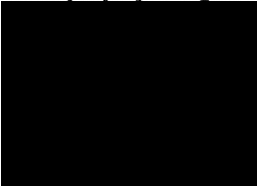
The notes on pages 6 to 7 form part of these financial statements.

Selkirk Means Business Ltd

Statement of financial position (continued)
31 March 2022

These financial statements have been prepared in accordance with the provisions applicable to companies subject to the small companies' regime and in accordance with Section 1A of FRS 102 'The Financial Reporting Standard applicable in the UK and Republic of Ireland'.

These financial statements were approved by the board of directors and authorised for issue on 20 December 2022, and are signed on behalf of the board by:



Stuart Davidson
Director

Company registration number: SC591540

The notes on pages 6 to 7 form part of these financial statements.

Selkirk Means Business Ltd

Statement of changes in equity (continued)
Year ended 31 March 2022

	Profit and loss account £	Total £
At 1 April 2020	328	328
Loss for the year	(110)	(110)
Total comprehensive income for the year	<u>(110)</u>	<u>(110)</u>
At 31 March 2021 and 1 April 2021	<u>218</u>	<u>218</u>
Loss for the year	(110)	(110)
Total comprehensive income for the year	<u>(110)</u>	<u>(110)</u>
At 31 March 2022	<u>108</u>	<u>108</u>

Selkirk Means Business Ltd

**Notes to the financial statements
Year ended 31 March 2022**

1. General information

The company is a private company limited by guarantee, registered in Scotland.
The address of the registered office is 15 High Street, Selkirk, TD7 4BZ.

2. Statement of compliance

These financial statements have been prepared in compliance with the provisions of FRS 102, Section 1A, 'The Financial Reporting Standard applicable in the UK and Republic of Ireland'.

3. Accounting policies

Basis of preparation

The financial statements have been prepared on the historical cost basis, as modified by the revaluation of certain financial assets and liabilities and investment properties measured at fair value through profit or loss.

The financial statements are prepared in sterling, which is the functional currency of the entity.

Turnover

Income comprises levies and grants received.

Tangible assets

Tangible assets are initially recorded at cost, and are subsequently stated at cost less any accumulated depreciation and impairment losses.

Any tangible assets carried at revalued amounts are recorded at the fair value at the date of revaluation less any subsequent accumulated depreciation and subsequent accumulated impairment losses.

Depreciation

Depreciation is calculated so as to write off the cost or valuation of an asset, less its residual value, over the useful economic life of that asset as follows: 20% straight line.

4. Project manager costs

	2022	2021
	£	£
Project manager costs	8,661	8,417

Selkirk Means Business Ltd

Notes to the financial statements (continued)
Year ended 31 March 2022

6. Tangible assets	Equipment	Total
	£	£
Cost		
At 1 April 2021 and 31 March 2022	548	548
	<hr/>	<hr/>
Depreciation		
At 1 April 2021	330	330
Charge for the year	110	110
	<hr/>	<hr/>
At 31 March 2022	440	440
	<hr/>	<hr/>
Carrying amount		
At 31 March 2022	108	108
	<hr/>	<hr/>
At 31 March 2021	218	218
	<hr/>	<hr/>
7. Debtors	2022	2021
	£	£
Other debtors	4,100	10,328
	<hr/>	<hr/>
8. Creditors: amounts falling due within one year	2022	2021
	£	£
Other creditors	19,069	28,030
	<hr/>	<hr/>

Selkirk Means Business Ltd**Detailed income statement
Year ended 31 March 2022**

	2022	2021
	£	£
Turnover		
Levies received	18,489	8,891
Grants and donations received	2,750	38,150
Shop Front Scheme	-	21,000
	<u>21,239</u>	<u>68,041</u>
Cost of sales		
Direct costs - SBC fee	(2,500)	(1,250)
	<u>(2,500)</u>	<u>(1,250)</u>
Gross profit	<u>18,739</u>	<u>66,791</u>
Overheads		
Administrative expenses		
Project manager fees	(8,661)	(8,417)
Project funds brought forward	11,022	10,946
Project funds spent	(2,466)	(32,510)
Project funds carried forward	(18,163)	(11,022)
Shop Front Scheme	-	(15,025)
Shop Front Scheme C/F	-	(5,975)
PPE	-	(4,205)
Printing, post & stationery	(363)	(213)
PM phone & travel expenses	(108)	(236)
Subscriptions	-	(134)
Depreciation of tangible assets	(110)	(110)
	<u>(18,849)</u>	<u>(66,901)</u>
Loss before taxation	<u>(110)</u>	<u>(110)</u>

SELKIRK BIDS – DATA PROTECTION COMPLAINTS POLICY 30.01.23

1 - Introduction

The General Data Protection Regulation (“GDPR”), the Data Protection Act 2018 (“DPA 2018”), and the Privacy and Electronic Communications Regulations (“PECR”) (together, the “Data Protection legislation”), give data subjects and applicable third parties rights in relation to personal data. This procedure details how Selkirk BIDS will respond to complaints from data subjects and third parties relating to the use of personal data

Who are Data Subjects?

Data subjects are any natural living individuals whose personal data Selkirk BIDS processes (collects, obtains, stores, retains, disposes of etc.). Data subjects can include volunteer/staff members, prospective applicants, visitors, individuals captured by the Selkirk BIDS’s CCTV cameras, etc.

Data subjects’ rights

Under Data Protection legislation, data subjects have the right to the following and these rights can be exercised at any time:

- information about the processing of their data
- access their own personal data
- correct personal data
- erase personal data, also known as the right to be forgotten
- restrict data processing
- object to data processing, including direct marketing
- receive a copy of their personal data or transfer their personal data to another data
- not be subject to automated decision-making and rights in relation to
- profiling
- be notified of a data security breach

What is a complaint?

A complaint is an expression of dissatisfaction about the Selkirk BIDS’s handling of a data subject’s personal data or the data of the individual they represent. This can also include dissatisfaction with how Selkirk BIDS has responded to a previous data request, such as those detailed under Data Subjects rights.

2 - Scope

This procedure addresses complaints made by data subjects regarding the use of their personal data. Complaints may be made in relation to any aspect of the Selkirk BIDS’s processing of personal data including individual rights requests.

This procedure also addresses complaints made by third parties in relation to the Selkirk BIDS’s use of personal data. These may be for example in relation to the NDCC’s response to a data related request from a third party, such as the Police or Local Government Agencies.

This procedure should also be followed for complaints in relation to use of personal data for direct marketing and/or profiling activity.

SELKIRK BIDS – DATA PROTECTION COMPLAINTS POLICY 30.01.23

3 - Responsibilities

Selkirk BIDS has overall responsibility for this procedure but has delegated day-to-day responsibility for overseeing its implementation to the Data Protection Officer. All relevant members of Selkirk BIDS have been made aware of the procedure and have received appropriate training. All nominated staff accessing CCTV will be Disclosure Checked in accordance with current Legislation.

All Volunteers/Staff are responsible for ensuring that any complaints that are made in relation to this procedure are reported to the Data Protection Officer/Data Protection Team (DAVCANDERSON@AOL.COM), and for cooperating with the Data Protection Officer in reviewing these complaints.

The Data Protection Officer and the Selkirk BIDS Board will review this procedure from time to time (and at least every two years) to ensure that its provisions continue to meet our legal obligations and reflect best practice.

4. Making a Complaint

Data subjects and third parties may make a complaint relating to the Selkirk BIDS use of personal data. Complaints should be sent directly to the Data Protection Officer/Team at (DAVCANDERSON@AOL.COM). A member of the Data Protection Team will normally acknowledge the complaint within 5 working days. Selkirk BIDS reserves the right to extend the period we need for response during vacation and Selkirk BIDS closure.

Although a complaint may be brought at any time, there may be limits as to what Selkirk BIDS can do in historic cases.

Selkirk BIDS will only accept a complaint from a data subject's representative, if the representative provides the data subject's written consent authorising the representative to act on the data subject's behalf in relation to the complaint.

If there is any doubt about the identity of the complainant, the Data Protection Team will first seek to verify the data subject's identity or third party's entitlement to act on behalf of the individual. The forms of identification that are acceptable from a data subject are as follows;

- a. Passport
- b. Driving Licence
- c. For third parties the identification requirements will vary dependent on their relationship to the data subject. Therefore these will be assessed on a case by case basis.

5 - Investigation and Complaint Outcome

Once all identification requirements have been met, the investigation will be carried out normally within 20 working days. If further clarification is required from the complainant or more time is required for the response to be completed Selkirk BIDS will inform the complainant prior to the original deadline.

The complaint outcome will be communicated to the complainant in writing, normally by email.

SELKIRK BIDS – DATA PROTECTION COMPLAINTS POLICY 30.01.23

6 - Review

If the complainant does not agree with the outcome, they can request a review of the decision. This request must be made within 1 month of the original decision being communicated and should be sent to the Data Protection Officer/Team at (DAVCANDERSON@AOL.COM).. The decision will be internally reviewed by the Data Protection Officer or Board normally within 20 working days from the receipt of the request for Review.

Once the internal review has been completed, Selkirk BIDS will communicate the outcome in writing, normally by email

Independent External Review

If the complainant remains dissatisfied, they can escalate their complaint to the Information Commissioner's Office (the "ICO"). Information about how to make a complaint to the ICO can be found here:

<https://ico.uk/make-a-complaint/>

In order to respond to the complaint, the Data Protection Officer will investigate the complaint based on the information provided by the ICO. This may necessitate access to personal data and other information held across Selkirk BIDS. The cooperation of any staff members able to assist with the investigation will be required. The reason for the investigation may need to be disclosed to the relevant volunteer/staff members.

The Data Protection Officer will draft and submit a response to the ICO in consultation with the Selkirk BIDS Board and Legal resources where appropriate.

In the absence of the Data Protection Officer, the Selkirk BIDS Board will appoint another member of the Data Protection and Information Compliance or Legal resources to carry out the investigation and respond to the ICO.

In some scenarios Selkirk BIDS can refuse to handle the complaint. This will be when a complaint is deemed to be manifestly unfounded, abusive, vexatious or excessive. Each complaint will be considered on a case by case basis. The following factors will be taken into consideration:

- the data subject has explicitly stated that they intend to cause disruption
- (whether in the complaint, or in other correspondence), and has threatened individuals
- the data subject has made unsubstantiated accusations against individuals, and is persisting in those accusations
- the data subject is targeting particular individuals, against whom they have a personal grudge;
- the data subject makes frequent complaints intended to cause disruption
- the data subject continues to repeat the substance of previous complaints which have already been investigated.

Where a complaint is deemed to be manifestly unfounded, excessive, abusive or vexatious Selkirk BIDS will contact the individual and in a reasonable timeframe explain to them:

- the reasons for refusing to consider the complaint
- their right to make a complaint to the ICO

SELKIRK BIDS – DATA PROTECTION COMPLAINTS POLICY 30.01.23

- their right to pursue their data subject rights through a judicial remedy

9 - Use of Data from Complaints

9.1. Selkirk BIDS will collect data on complaint outcomes at each stage of this procedure and any complaints submitted by complainants to any regulators (including the ICO), and use the data: a) internally for reporting, evaluation, learning and training; and b) externally for discussion with regulators

9.2. The data used by Selkirk BIDS for the purposes set out in paragraphs 9.1 a) and b) will be anonymised. Your personal data and sensitive personal data ('Personal Data') as defined by the Data Protection Act 2018 (the "DPA") may be disclosed to Selkirk BIDS's members of staff and regulators only for the purpose of dealing with your complaint, or a complaint arising out of it and/or implementing any recommendations. Personal Data will not be shared with any other third parties unless Selkirk BIDS has your express consent, has a statutory obligation to do so, or is otherwise permitted to do so under the DPA.

FURTHER HELP AND ADVICE

For more information and advice about this policy contact

Data Protection Officer

Selkirk BIDS

48 High Street

Selkirk

TD7 4DD

Email: DAVCANDERSON@AOL.COM

Web: <https://www.exploreselkirk.co.uk>

ICO Scotland contact details

The Information Commissioner's Office – Scotland

Queen Elizabeth House

Sibbald Walk

Edinburgh

EH8 8FT

Telephone: 0303 123 1115

Email: Scotland@ico.org.uk



**SURVEILLANCE CAMERA
COMMISSIONER**

ico.
Information Commissioner's Office

Data protection impact assessments template for carrying out a data protection impact assessment on surveillance camera systems

Project name:

Data controller(s): SECRETARY: BARBARA ELBORN
NEWCASTLETON DISTRICT COMMUNITY COUNCIL

This DPIA template should be completed with reference to the guidance provided by the Surveillance Camera Commissioner and the ICO. It will help you to identify whether the use of surveillance cameras is appropriate for the problem you wish to address, assess the risks attached to your project and form a record of your decision making.

1. Identify why your deployment of surveillance cameras requires a DPIA¹:

- | | |
|---|--|
| <input type="checkbox"/> Systematic & extensive profiling | <input type="checkbox"/> Large scale use of sensitive data |
| <input checked="" type="checkbox"/> Public monitoring | <input type="checkbox"/> Innovative technology |
| <input type="checkbox"/> Denial of service | <input type="checkbox"/> Biometrics |
| <input type="checkbox"/> Data matching | <input type="checkbox"/> Invisible processing |
| <input type="checkbox"/> Tracking | <input type="checkbox"/> Targeting children / vulnerable adults |
| <input checked="" type="checkbox"/> Risk of harm | <input checked="" type="checkbox"/> Special category / criminal offence data |
| <input type="checkbox"/> Automated decision-making | <input checked="" type="checkbox"/> Other (please specify) |

2. What are the timescales and status of your surveillance camera deployment? Is this a proposal for a new deployment, or the expansion of an existing surveillance camera system? Which data protection regime will you be processing under (i.e. DPA 2018 or the GDPR)?

Newcastleton Public Space Close Circuit TV (CCTV) system will be owned and operated by Newcastleton & District Community Council.
This will be a new system which covers key local assets and roadways in 8 locations in Newcastleton. Handling of images and information within the Control Room will be carried out in accordance with the Data Protection Act 2018

Describe the processing

3. Where do you need to use a surveillance camera system and what are you trying to achieve?

Set out the **context** and **purposes** of the proposed surveillance cameras or the reasons for expanding an existing system. Provide evidence, where possible, including for example: crime statistics over an appropriate time period; housing and community issues, etc.

The 'Public Space CCTV system' will have 8 cameras situated at locations covering key local assets and roadways in Newcastleton.
The NDCC CCTV surveillance system has been installed and is monitored for the following purposes:

- Provides a series of linked cameras for all entrances to our village as well as capture locations prone to regular vandalism (school, Polysport, riverside).
- Reduces the likelihood of the village being used as a thoroughfare for criminal activity

¹ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/>

- Reduces the likelihood of local and regional 'cruising' groups using the village as a racetrack
- Reduces the likelihood of criminal gangs using the forest roads as a getaway between Central Scotland and North East England.
- Provides 'remote live views' for our resilience team and SBC Emergency bunker to see real time events on the river Liddel.
- Captures footage over time to help understand changing river behaviours, using the findings to refine the flood scheme.
- Provides a 20-minute warning to residents to try to avoid the devastation Storm Dennis caused in Feb 2020 with a further flood event in Feb 20201 causing substantial damage within the community.

4. Whose personal data will you be processing, and over what area? Set out the **nature** and **scope** of the personal data you will be processing. Who are the data subjects, and what kind of information will you be collecting about them? Do they include children or vulnerable groups, and what is the scale and duration of the processing?

The personal data being processed will primarily be of members of the public while they are in the the general area of Newcastleton village.

The movements of some vulnerable individuals may be captured in some instances, and as the primary purpose of the system is to reduce, detect or prevent crime, disorder or anti-social behaviour or vandalism and the movements of offenders and victims will also be captured. Movement of young people will also be captured in some instances.

The general public will easily be aware that CCTV is monitoring the areas as there are a number of clear signs and warnings that CCTV is in use.

The use of the system will remain in line with the list of objectives in the Code of Practice.

Images are retained on the system for 28 days from the point of recording; unless required for evidential purposes, the images are automatically deleted at that point. Images provided for evidential purposes are kept until notification is received that they are no longer required. Images relating to flooding will be held for a period of 90 days.

The use of CCTV is deemed proportionate and not in conflict with Human Rights Act 1998.

5. Who will be making decisions about the uses of the system and which other parties are likely to be involved? Will you be the sole user of the data being processed or will you be sharing it with other organisations or agencies? Record any other parties you would disclose the data to, for what purposes, and any relevant data sharing agreements. Note that if you are processing for more than one purpose you may need to conduct separate DPIAs.

Who will be making decisions about the uses, NDCC Community Council have responsibility for systems and will be only be sharing the data with Nominated persons as indicated in our policies. Those being Chair of NDCC, Chair of Resilience Group, and NDCC Data Controller. Information would only be shared with organisations ie Police or other SIA approved persons.

6. How is information collected? (tick multiple options if necessary)

- | | |
|--|---|
| <input checked="" type="checkbox"/> Fixed CCTV (networked) | <input type="checkbox"/> Body Worn Video |
| <input type="checkbox"/> ANPR | <input type="checkbox"/> Unmanned aerial systems (drones) |
| <input type="checkbox"/> Stand-alone cameras | <input type="checkbox"/> Redeployable CCTV |
| <input type="checkbox"/> Other (please specify) | |

7. Set out the information flow, from initial capture to eventual destruction. You may want to insert or attach a diagram. Indicate whether it will include audio data; the form of transmission; the presence of live monitoring or use of watchlists; whether data will be recorded; whether any integrated surveillance technologies such as automatic facial recognition are used; if there is auto deletion after the retention period. You may have additional points to add that affect the assessment.

Images captured by cameras will be collected and recorded on equipment via our encrypted data network, located securely within Buccleuch House (Control Room). The Control Room has monitoring equipment which has the capability of monitoring live images from the cameras. This operation is disabled from viewing and can only be used in the event there is a justification for doing so, an example of this will be a specific request from the police, and the appropriate completion of documentation to support this will be undertaken. Transfer of images onto other media will only take place from within the Control Room in line with these procedures. The Control Room is supported by a digital recording system which stores images on appropriate media for 28 days or until capacity is reached, and the images are then automatically erased. The exception to the 28 days of image storing will be flood images, which will be 90 days. The system recording and images are capable of being monitored twenty-four hours a day throughout the year. All CCTV cameras are configured to record images only: any sound recording facilities will be switched off or disabled. We currently do not have any automatic facial recognition software.

8. Does the system's technology enable recording?

- Yes No

If recording is enabled, state where it is undertaken (no need to stipulate address, just Local Authority CCTV Control room or on-site will suffice for stand-alone camera or BWV), and whether it also enables audio recording.

Buccleuch House is the location where recording is enabled, but non audio

9. If data is being disclosed, how will this be done?

- Only by on-site visiting
 Copies of footage released (detail method below, e.g. encrypted digital media, via courier, etc)
 Off-site from remote server
 Other (please specify)

If any information is required; a formal request must be made in writing via the appropriate department using our official Access Request forms. These are then checked and authorised by our Data Protection Officer. A review is then carried out by a fully trained CCTV operator in our secure facility. If anything is found it will then be burned and encrypted onto a disc. The department that requested the review will then be notified in writing regarding completion and a collection date and time will be agreed. On agreed arrival for the collection of encrypted data, the responsible party will show identification before being allowed access to our secure facility. They will then be entered into our operators log to ensure we have a record of their arrival and departure in written format. The identified party will then need to sign the relevant release papers; they are then free to take the evidence from the building.

10. How is the information used? (tick multiple options if necessary)

- Monitored in real time to detect and respond to unlawful activities
- Monitored in real time to track suspicious persons/activity
- Compared with reference data of persons of interest through processing of biometric data, such as facial recognition.
- Compared with reference data for vehicles of interest through Automatic Number Plate Recognition software
- Linked to sensor technology
- Used to search for vulnerable persons
- Used to search for wanted persons
- Recorded data disclosed to authorised agencies to support post incident investigation, including law enforcement agencies
- Recorded data disclosed to authorised agencies to provide intelligence
- Other (please specify)

Consultation

11. Record the stakeholders and data subjects you have consulted about the deployment, together with the outcomes of your engagement.

Stakeholder consulted	Consultation method	Views raised	Measures taken
Community	Written consultation	Supportive donations to the CCTV project plus agreement from community households and business to permit the use of their premises to position cameras on their properites	Documented
Scottish Border Council	Written consultation	Supportive planning application and the proposed use to detect crime, together with assisting with flooding	Documented
Police Scotland	Written consultation	Supportive of proposal of the scheme	Documented

--	--	--	--

Consider necessity and proportionality

12. What is your lawful basis for using the surveillance camera system? Explain the rationale for your chosen lawful basis under the relevant data protection legislation. Consider whether you will be processing special categories of data.

Newcastleton & District Community Council is fully compliant with the lawful reasons for processing Personal Data, as detailed under Schedule 2 of the Data Protection Act 2018: •

Processing is necessary for the purposes of legitimate interests pursued by the appointed Data Controller and third-party discloser's and does not prejudice the rights and freedoms and legitimate interests of others and with the lawful reasons for processing Sensitive Personal Data, under Schedule 3 of the Act, wherein the process:

- Is in the substantive public interest.
- Is necessary for the purposes of the prevention and detection of any unlawful act.
- Must necessarily be carried out without the explicit consent of the data subjects so as not to prejudice those purposes.

13. How will you inform people that they are under surveillance and ensure that they are provided with relevant information? State what privacy notices will be made available and your approach to making more detailed information available. Consider whether data subjects would reasonably expect to be under surveillance in this context.

The public and community will be made aware of the presence of the system by appropriate ICO approved signage which sets out the purposes for processing the CCTV images and identifies the NDCC as the Data Controller responsible for processing those images
Obviously a number of residents will have legitimate concerns regarding the use to which CCTV is put. By ensuring compliance with current legislation we hope to show that the CCTV camera system is only used for the detection and reduction of crime and activities that ultimately assist the public. We have not received any complaints regarding the use of CCTV. The community is engaged via various local organisations with good support from them
Subject Access Requests, Privacy Notices and Complaints will detailed on the Visit Newcastleton website and in written format.

14. How will you ensure that the surveillance is limited to its lawful purposes and the minimum data that is necessary for those purposes? Explain the adequacy and relevance of the data you will be processing and how it is limited to the purposes for which the surveillance camera system will be deployed. How will you know if it is delivering the benefits it has been deployed for?

The surveillance is all activities, processes, procedures that incorporate the management, monitoring, reviewing, and storing of CCTV images.

The objectives of the system as determined by Newcastleton & District Community Council forming the lawful basis for the processing of this data are:

- For the purposes of monitoring river levels for flood prevention.
- Water safety and management.
- Prevention, investigation, and detection of crime.
- To help with the increased apprehending and prosecution of offenders.
- Risk management and environmental concerns.
- Increase in public safety and public reassurance

NDCC will ensure operators of the CCTV are fully trained to understand the objectives of the system, and the lawful basis for collecting data for the purpose detailed in our Code of Conduct.

Images must be adequate for the purpose of the system. For the prevention and detection of crime, the images should be capable of identifying individuals who may be suspects or witnesses to a criminal offence. This would include clothing, vehicle make and model and include registration numbers. For general public safety monitoring, the majority of images would be unidentifiable in relation to personal data unless the camera was being used to monitor an incident.

We will audit our system and produce regular data reports showing the benefits of the system to ensure it stays relevant for the elements outlined in our Codes of Practice.

15. How long is data stored? (please state and explain the retention period)

The Control Room is supported by a digital recording system which stores images on appropriate media for 28 days and the images are then automatically erased. Recording for the purpose of flood management will be stored for 90 days

16. Retention Procedure

- Data automatically deleted after retention period
- System operator required to initiate deletion
- Under certain circumstances authorised persons may override the retention period, e.g. retained for prosecution agency (please explain your procedure)

In the case where recordings are retained for prosecution agencies, The Operations Manager will liaise with the police to ensure that the NDCC is informed of the outcome of the police investigation and authorise the police to destroy any NDCC CCTV images and recordings when they are no longer required

17. How will you ensure the security and integrity of the data? How is the data processed in a manner that ensures appropriate security, protection against unauthorised or unlawful processing and against accidental loss, destruction or damage? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

NDCC have taken steps to implement our Security Policy and we have additional policies including training, code of conduct, privacy policies in place to enforce them. These policies have been assessed by the Community Council, and what we need to do by considering the security outcomes we want to achieve.

Privacy Zones are programmed on cameras where appropriate preventing any intentional or accidental intrusion into residential property.

We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process. We use encryption in our communication where it is appropriate to do so.

NDCC has policies in place which covers volunteers/staff requirements of confidentiality, integrity and availability for the personal data we process. We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.

NDCC conducts regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement. Where appropriate, we implement measures that adhere to our code of conduct. We ensure that any data processor we use also implements appropriate technical and organisational measures.

18. How will you respond to any subject access requests, the exercise of any other rights of data subjects, complaints or requests for information? Explain how you will provide for relevant data subject rights conferred under the legislation. You must have procedures in place to respond to requests for camera footage in which a subject appears, and to respond to any other request to meet data protection rights and obligations.

Subject Access Requests, Privacy Notices and Complaints Procedures will be listed on VIsit Newcastleton website and available if required in written format.

19. What other less intrusive solutions have been considered? You need to consider other options prior to any decision to use surveillance camera systems. For example, could better lighting or improved physical security measures adequately mitigate the risk? Does the camera operation need to be continuous? Where you have considered alternative approaches, provide your reasons for not relying on them and opting to use surveillance cameras as specified.

Other solutions are always considered including the use of additional resources such as preventative work and to work with other agencies and / or private businesses as appropriate before CCTV is installed.

20. Is there a written policy specifying the following? (tick multiple boxes if applicable)

The agencies that are granted access

How information is disclosed

How information is handled

Are these procedures made public? Yes No

Are there auditing mechanisms? Yes No

If so, please specify what is audited and how often (e.g. disclosure, production, accessed, handled, received, stored information)

Codes of Practice and Self Assessment of the system is undertaken on an annual basis. Procedures are altered in response to other factors such as the Covid-19 pandemic which has stopped access to the Control Room to all but the operators who are required to be in the Control Room. The Operators Manual is reviewed on a two-yearly basis or as individual processes are required to change.

Identify the risks

Identify and evaluate the inherent risks to the rights and freedoms of individuals relating to this surveillance camera system. Consider, for example, how long will recordings be retained? Will they be shared? What are the expectations of those under surveillance and impact on their behaviour, level of intrusion into their lives, effects on privacy if safeguards are not effective? Could it interfere with other human rights and freedoms such as those of conscience and religion, expression or association. Is there a risk of function creep? Assess both the likelihood and the severity of any impact on individuals.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
Automatic deletion of images does not occur leading to images being kept longer than stated time period within the Codes of Practice	Remote, possible or probable Remote	Minimal, significant or severe Minimal	Low, medium or high Low
Operators monitor individuals inappropriately – outside of normal working practices, in breach of codes of conduct etc	Remote	Minimal	Low
Images are inappropriately shared on social media sites by Operators	Remote	Significant	Low
Access by unauthorised persons into the Control Room	Remote	Minimal	Low

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
Operators are able to monitor behaviour in individual's homes	Remote, possible or probable Remote	Minimal, significant or severe Significant	Low, medium or high Low

Address the risks

Explain how the effects of privacy enhancing techniques and other features mitigate the risks you have identified. For example, have you considered earlier deletion of data or data minimisation processes, has consideration been given to the use of technical measures to limit the acquisition of images, such as privacy masking on cameras that overlook residential properties? What security features, safeguards and training will be in place to reduce any risks to data subjects. Make an assessment of residual levels of risk.

Note that APPENDIX ONE allows you to record mitigations and safeguards particular to specific camera locations and functionality.

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk			
Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved?
System is checked regularly to ensure that deletion takes place as per the automatic settings	Eliminated reduced accepted Eliminated	Low medium high Low	Yes/no Yes
Training is undertaken, operators are checked, regular 121s take place, management auditing undertaken of patrols	Eliminated	Low	Yes
Access points are monitored by management, use of visitor book/Operators log is mandatory, room is locked when operators are not in the control room and live screens switched off.	Eliminated	Low	Yes

Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved?
Training is undertaken, and operators are checked, privacy panels are installed on each camera that may provide the opportunity for images to recorded from within people's homes	Eliminated reduced accepted Eliminated	Low medium high Low	Yes/no Yes

Authorisation

If you have not been able to mitigate the risk then you will need to submit the DPIA to the ICO for prior consultation. [Further information](#) is on the ICO website.

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by:		If you identify a high risk that you cannot mitigate adequately, you must consult the ICO before starting to capture and process images.
DPO advice provided by:		DPO should advise on compliance and whether processing can proceed.
Summary of DPO advice		
DPO advice accepted or overruled by: (specify role/title)		If overruled, you must explain your reasons.
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons.
Comments:		
This DPIA will be kept under review by: B Elborn		The DPO should also review ongoing compliance with DPIA.

APPENDIX ONE

This template will help you to record the location and scope of your surveillance camera system and the steps you've taken to mitigate risks particular to each location.

Location: Each system operator/owner should list and categorise the different areas covered by surveillance on their system. Examples are provided below.

Location type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
Location 1 South end of Village Polysport, camperdown TD9 0TA	Bullet/Turret	8Mp	24hrs	Unmanned 24hrs recording – Limited due to the fact that most are static cameras 28 day data storage	The privacy level expectation in the area is very low; the community are well signed with appropriate signage for CCTV its use and purpose with contact details
Location2. Dalkeith House, TD9 0QD	Bullet/Turret	8Mp	24hrs	Unmanned 24hrs recording – Limited due to the fact that most are static cameras 28 day data storage	The privacy level expectation in our Main Square is very low; our community is well signed with appropriate signage for CCTV its use and purpose with contact details
Location3. Grapes Hotel, TD9 0QD	180 degree	8Mp	24hrs	Unmanned 24hrs –Limited due to the fact that most are static cameras 28 day data storage	The privacy level expectation in our Main Square is very low; our community is well signed with appropriate signage for CCTV its use and purpose with contact details
Location 4. Spar / Post Office, TD9 0RB	180 degree	8Mp	24hrs	Unmanned 24hrs –Limited due to the fact that most are static cameras 28 day data storage	The privacy level expectation in our Main street is very low; our community is well signed with appropriate signage for CCTV its use and purpose with contact details
Location 5 Community Fuel station Td9 0DZ	Bullet/Turret	8Mp	24hrs	Unmanned 24hrs –Limited due to the fact that most are static cameras 28 day data storage	The privacy level expectation in our Main street is very low; our community is well signed with appropriate signage for CCTV its use and purpose with contact details
Location 6. Whithaugh Pool Community Recreation Land	Bullet/Turret	8Mp	24hrs	Unmanned 24hrs –Limited due to the fact that most are static cameras	The privacy level expectation in the area is very low; the community are well signed with appropriate signage for

Location type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
				90 day data storage	CCTV its use and purpose with contact details
Location 7 Village Primary School, TD9 0QZ	Bullet/Bullet	8Mp	24hrs	Unmanned 24hrs –Limited due to the fact that most are static cameras 28 day data storage	The privacy level expectation in our school grounds is very low; our community is well signed with appropriate signage for CCTV its use and purpose with contact details

APPENDIX TWO: STEPS IN CARRYING OUT A DPIA



APPENDIX THREE: DATA PROTECTION RISK ASSESSMENT MATRIX

Use this risk matrix to determine your score. This will highlight the risk factors associated with each site or functionality.

Matrix Example:

	Camera Types (low number low impact – High number, High Impact)									
	→									
Location										
Types										
A (low impact)										
Z (high impact)										

NOTES

This page is intentionally left blank

**SELKIRK BIDS
CCTV ACCESS PERMISSIONS**

Appointed and Trained Selkirk BIDS appointees

Mr David Anderson
Chair of Selkirk BIDS

Mr Stuart Davidson
Director of Selkirk BIDS

Mrs Vivienne Ross
Director of Selkirk BIDS

Data Controller

Mr David Anderson
Director of Selkirk BIDS

This page is intentionally left blank

SELKIRK BIDS RIGHT OF ACCESS POLICY 30.01.23

Individuals have the right to ask whether, or not, Selkirk BIDS are using or storing their personal information. They can ask for copies of their personal information, verbally or in writing.

This is called the right of access and is commonly known as making a subject access request or SAR.

This policy explains how to respond to a subject access request.

Individuals can make a subject access request to find out:

- what personal information Selkirk BIDS holds about them
- how we are using it
- who we are sharing it with
- where we got their data from

When Selkirk BIDS responds to requests, they should normally explain whether or not they process individual's personal information and, if they do, give them copies of it. This information should also include (where applicable):

- what we are using individual's information for
- who we are sharing this information with
- how long we will store this information, and how we made this decision
- details on individual's rights to challenge the accuracy of Selkirk BIDS information, to have it deleted, or to object to its use
- individual's rights to complain to the ICO
- details about where we got individual information from
- whether we use individual information for profiling or automated decision-making and how we are doing this; and
- what security measures we took if we have transferred individual's information to a third country or an international organisation.

How long does an organisation have to respond?

As an organisation Selkirk BIDS normally will respond to a request within 40 days.

The Operations Manager is responsible for documenting each request.

All nominated staff will be Disclosure Checked in accordance with current Legislation.

SELKIRK BIDS RIGHT OF ACCESS POLICY 30.01.23

CCTV

All requests for CCTV access will be recorded using the Selkirk BIDS Disclosure Decision form [Appendix C D] detailing:

- the date, time and purpose of the request
- the decision to release or withhold the images and the reasons for the decision in each case
- the date and time at which access was allowed/or disclosure made
- the extent of the information accessed/ or disclosed
- the name and role of the Data Protection officer making the decision to allow or withhold access
- the name of the nominated person providing access.

Selkirk BIDS must comply with section 7 of the Data Protection Act, 2018, in informing individuals whether or not images and other information relating to them have been processed by the CCTV Surveillance System. Individuals whose images are recorded have a right to make a request to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images.

In order to comply with a request, Selkirk BIDS needs to satisfy itself as to the identity of the person making the request for their own personal data. The person making the request also needs to provide enough information to enable Selkirk BIDS staff to locate their images. Therefore, Data Subjects wishing to make a subject access request (request for data about themselves) for CCTV images / recordings / information must apply in writing to the Data Protection Officer at the address given at the end of this Procedure.

In the request, the requestor must provide the following information

- Dates and times of the incident or their visit to Selkirk BIDS with details of the location.
- TWO pieces of ID (e.g. driving licence/passport containing a photograph); one of these must show the applicants current address proof of identity (e.g. driving licence/passport containing a photograph);
- Payment of the sum of £10.00;
- Whether they require copies or view of the images in question.

A written decision will be sent to the data subject within 14 working days of receipt of the request. If access is agreed, such access will be provided within forty days of receipt of the request or, if later, on the date when Selkirk BIDS receives confirmation of identification from the data subject.

In responding to a subject access request, Selkirk BIDS staff will use red action tools to obscure images of other individuals in cases where, releasing the unredacted images would involve an unfair intrusion into the privacy of the third parties concerned. Where Selkirk BIDS is unable to comply with a subject access request without disclosing information relating to another individual who can be identified from that information, it is not obliged to comply with the request unless that individual

SELKIRK BIDS RIGHT OF ACCESS POLICY 30.01.23

has consented to the disclosure or it is reasonable, in the circumstances, to comply without the consent of the individual.

Access by the Police

A police officer may request access to CCTV images held by Selkirk BIDS either by viewing such data within the Control Room at 48 High Street or requesting a copy of the data. In most cases the police will request such access in response to a request by Selkirk BIDS to investigate an alleged offence. In cases where the police request Selkirk BIDS CCTV footage to investigate an alleged offence that the Selkirk BIDS has not reported, such requests for access to images are subject to the approval process set out in the Procedures for Liaison with Police.

During working hours, requests for CCTV footage should be referred to the Data Protection Officer

Outside of working hours requests for access to images should wherever possible be deferred until they can be considered by the appropriate Data Protection officer during working hours. In an emergency, if a request is straightforward and justifiable, for instance, a request for images of one incident involving criminal activity such as theft of a vehicle or equipment, the Operations Manager or nominated person may authorise disclosure to the police provided that:

- the request is in writing using the appropriate form (Appendix A) signed by a Senior Police Officer, who must cite the relevant exemption/s to the non-disclosure provisions of the Data Protection Act; and
- the police demonstrate that the request is proportionate and necessary for the purposes of a specific crime enquiry. In all other cases the Operations Manager or nominated person will report the request to the Data Controller to seek authorisation to take appropriate action. These procedures will be supported by underpinning guidance which will set out examples of straightforward and justifiable requests and those requiring escalation.

The Operations manager will complete form to confirm the authenticity of the recordings and arrange for all data on recordings required for disclosure to be copied onto secure encrypted media.

The Operations manager must complete details of the request and any disclosure made in the Incident Report in the Selkirk BIDS's Safeguard electronic recording system. For each disclosure request, a copy of the completed police request form, including the reasons given for the request, together with a Selkirk BIDS Disclosure Decision form [Appendix C] recording the decision to withhold or release the information, an encrypted copy of the recording disclosed, where applicable, and reasons for the decision must be lodged with the following responsible officers who maintain a complete confidential record of all such cases on behalf of the Data Protection officer.

Images and recordings requested for police investigations must be supplied directly to the police, not to any third party. Requests by individuals for their own images captured on CCTV will be dealt with in accordance with the section

The Operations Manager will liaise with the police to ensure that the Selkirk BIDS is informed of the outcome of the police investigation and authorise the police to destroy any Selkirk BIDS CCTV images and recordings when they are no longer required.

SELKIRK BIDS
RIGHT OF ACCESS POLICY 30.01.23

FURTHER HELP AND ADVICE

For more information and advice about this policy contact

Data Protection Officer

Selkirk BIDS

48 High Street

SELKIRK

TD7 4DD

Email: DAVCANDERSON@AOL.COM

Web: <https://www.exploreselkirk.co.uk>

ICO Scotland contact details

The Information Commissioner's Office – Scotland

Queen Elizabeth House

Sibbald Walk

Edinburgh

EH8 8FT

Telephone: 0303 123 1115

Email: Scotland@ico.org.uk

**SELKIRK BIDS
RIGHT OF ACCESS POLICY 30.01.23**

SUBJECT ACCESS REQUEST FORM

SELKIRK BIDS – CCTV

DATA PROTECTION ACT 2018

(incorporating the GDPR 2018)

How to Apply For Access To Information Held On the Selkirk BIDS – CCTV System

These notes explain how you can find out what information, if any, is held about you on the CCTV System. Please note that CCTV images are only retained for 28 days.

Your Rights

Subject to certain exemptions, you have a right to be told whether any personal data is held about you. You also have a right to a copy of that information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or if you agree otherwise. Selkirk BIDS will only give that information if it is satisfied as to your identity. If release of the information will disclose information relating to another individual(s), who can be identified from that information, the Council is not obliged to comply with an access request unless –

- The other individual has consented to the disclosure of information, or
- It is reasonable in all the circumstances to comply with the request without the consent of the other individual(s)

Selkirk BID's Rights

Selkirk BIDS may deny access to information where the Regulation allows. The main exemptions in relation to information held on the CCTV System are where the information may be held for: Prevention and detection of crime

- Apprehension and prosecution of offenders
- And giving you the information may be likely to prejudice any of these purposes.

Fee

A fee to deal with this request is £20.00 in most circumstances. Applications can be made using this form

The Application Form:

(NB all sections of the form must be completed. Failure to provide all the information may delay your application)

Section 1 Asks you to give information about yourself that will help the Council to confirm your identity. NDCC Council has a duty to ensure that information it holds is secure and it must be satisfied that you are who you say you are.

Section 2 Asks you to provide evidence of your identity by producing TWO official documents (which between them clearly show your name, date of birth and current address) together with a recent full-face photograph of you.

Section 3 Asks you to confirm whether you will accept just viewing the information, or if you want a copy of the information.

Section 4 You must sign the declaration

When you have completed and checked this form, take or send it together with the required TWO identification documents and photograph to:

CCTV Data Protection Officer, Selkirk BIDS, 48 High Street, Selkirk, TD7 4DD

Email Requests: These can be made direct to secretary@newcastletoncommunitytrust.co.uk

If you have any queries regarding this form, or your application, please email secretary@newcastletoncommunitytrust.co.uk

**SELKIRK BIDS
RIGHT OF ACCESS POLICY 30.01.23**

SELKIRK BIDS CCTV SURVEILLANCE SYSTEM				
DATA PROTECTION ACT 2018				
(incorporating the GDPR 2018)				
SECTION 1 About Yourself				
The information requested below is to help the Council (a) satisfy itself as to your identity and (b) find any data held about you.				
PLEASE USE BLOCK LETTERS				
Title (tick box as appropriate)	Mr	Mrs	Miss	Ms
Other title (e.g. Dr., Rev., etc.)				
Surname/family name				
First names				
Maiden name/former names				
Sex (tick box)	Male		Female	
Height				
Date of Birth				
Place of Birth	Town		County	
Your Current Home Address				
Post Code				
(to which we will reply)				
A telephone number will be helpful in case you need to be contacted.				
Tel. No.				
SECTION 2 Proof of Identity				
To help establish your identity your application must be accompanied by TWO official documents that between them clearly show your name, date of birth and current address.				
For example: a birth/adoption certificate, driving licence, medical card, passport or other official document that shows your name and address. Also a recent, full face photograph of yourself.				
Failure to provide this proof of identity may delay your application.				
SECTION 3 Supply of Information				
You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form. Do you wish to:				
(a) View the information and receive a permanent copy	YES/NO			
(b) Only view the information	YES/NO			
NOW – please complete Section 4 and then check the ‘CHECK’ box (on page 5) before returning the form.				
SECTION 4 Declaration				
DECLARATION (to be signed by the applicant)				
The information that I have supplied in this application is correct and I am the person to whom it relates.				
Signed by	Date			
Warning – a person who impersonates or attempts to impersonate another may be guilty of an offence.				



SELKIRK BIDS

COMMUNITY PROCEDURES – To support Information Security Policy Framework 30.01.23 COUNCIL

SUBJECT ACCESS REQUEST FORM APPENDIX C

SELKIRK BIDS – CCTV

DATA PROTECTION ACT 2018 (incorporating GDPR 2018)

This document should be completed after reading the CCTV procedures document

How to Apply For Access To Information Held On the Selkirk BIDS – CCTV System

These notes explain how you can find out what information, if any, is held about you on the CCTV System. Please note that CCTV images are only retained for 28 days.

Your Rights

Subject to certain exemptions, you have a right to be told whether any personal data is held about you. You also have a right to a copy of that information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or if you agree otherwise. Selkirk BIDS will only give that information if it is satisfied as to your identity. If release of the information will disclose information relating to another individual(s), who can be identified from that information, Selkirk BIDS is not obliged to comply with an access request unless –

- The other individual has consented to the disclosure of information, or
- It is reasonable in all the circumstances to comply with the request without the consent of the other individual(s)

Selkirk BIDSs Rights

Selkirk BIDS may deny access to information where the Regulation allows. The main exemptions in relation to information held on the CCTV System are where the information may be held for: Prevention and detection of crime

- Apprehension and prosecution of offenders
- And giving you the information may be likely to prejudice any of these purposes.

Fee

A fee to deal with this request is £10.00 in most circumstances. Applications can be made using this form

The Application Form: all sections of the form must be completed.

Section 1 Asks you to give information about yourself that will help confirm your identity. Selkirk BIDS has a duty to ensure that information it holds is secure and it must be satisfied that you are who you say you are.

Section 2 Asks you to provide evidence of your identity TWO pieces of ID (e.g. driving licence/passport containing a photograph); one of these must show your current address

Section 3 Asks you to confirm whether you will accept just viewing the information, or if you want a copy of the information.

Section 4 You must sign the declaration



SELKIRK BIDS

COMMUNITY COUNCIL PROCEDURES – To support Information Security Policy Framework 30.01.23

SUBJECT ACCESS REQUEST FORM APPENDIX D

SELKIRK BIDS CCTV SURVEILLANCE SYSTEM

DATA PROTECTION ACT 2018 (incorporating the GDPR 2018)

SECTION 1 About Yourself

The information requested below is to help Selkirk BIDS satisfy itself as to your identity and find any data requested

PLEASE USE BLOCK LETTERS

Title (tick box as appropriate) Mr Mrs Miss Ms

Other title (e.g. Dr., Rev., etc.)

Surname/family name

First names

Maiden name/former names

Your Current Home Address

Post Code

A telephone number will be helpful in case you need to be contacted.

Tel. No.

SECTION 2 Proof of Identity

To establish your identity your application must be accompanied by TWO pieces of ID (e.g. driving licence/passport containing a photograph); one of these must show your current address

SECTION 3 Supply of Information

You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form. Do you wish to:

(a) View the information and receive a permanent copy YES/NO

(b) Only view the information YES/NO

SECTION 4 Declaration

DECLARATION (to be signed by the applicant)

The information that I have supplied in this application is correct and I am the person to whom it relates.

Signed by _____

Date ____/____/____

Warning – a person who impersonates or attempts to impersonate another may be guilty of an offence.

PROCEDURES FOR OPERATION OF CCTV ON SELKIRK BIDS PREMISES TO SUPPORT INFORMATION SECURITY POLICY FRAMEWORK

CONTENTS

1 INTRODUCTION

2 SCOPE

3 OBJECTIVES

4 OPERATION OF THE NDCC'S CCTV SURVEILLANCE SYSTEM

5 MONITORING OF CCTV IMAGES

6 RECORDING OF IMAGES AND RESPONDING TO ACCESS REQUESTS

7 COMPLAINTS/BREACHES

8 RESPONSIBLE OFFICER

9 MONITORING AND REVIEW

10 RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

11 FURTHER HELP AND ADVICE

Appendix A - Access documents

SECTION 1 - INTRODUCTION

These procedures are applicable to all Selkirk BIDS staff or their nominated representatives. Their purpose is to ensure that the Selkirk BIDS Closed Circuit Television (CCTV) system is used to create a safer environment for residents, and visitors to Selkirk and to ensure that its operation is consistent with the obligations on Selkirk BIDS imposed by the Data Protection Act 2018.

For the purposes of the Data Protection Act 2018, the Data Controller is Selkirk BIDS. Selkirk BIDS has installed a comprehensive CCTV surveillance system across Selkirk for the principal purposes of preventing and detecting crime and promoting public safety.

The images from the CCTV system are located in 48 High Street, Selkirk (CCTV Operation Room).

It is recognised that ancillary benefits of operating CCTV for this purpose may include reduction of the fear of crime generally and the provision of a safer public environment for the benefit of those who live or work within and visit the town.

CCTV Cameras which are located on buildings are the responsibility of Selkirk BIDS who is accountable for compliance with these procedures. Following the introduction of these procedures a programme will be agreed to manage the migration of all Selkirk BIDS CCTV cameras onto a common platform which will allow all recordings to be monitored from 48 High Street, Selkirk.

Due to public concern surrounding a surveillance society, the use of CCTV surveillance must be consistent with respect for individuals' privacy. Other methods of achieving the objectives of a CCTV surveillance system will therefore be considered before installation of any CCTV camera positions.

SECTION 2 - SCOPE

These procedures apply to all Selkirk BIDS CCTV cameras and equipment across Selkirk. Selkirk BIDS is the Data Controller for this system, determines the purpose of recording and is legally responsible and accountable for its use. These procedures will be adapted to apply to all systems for which Selkirk BIDS is the Data Controller for all camera locations.

SECTION 3 - OBJECTIVES

Selkirk BIDS CCTV surveillance system has been installed and is monitored for the following purposes:

- Provides a series of linked cameras for all entrances to our town centre as well as capture locations prone to regular vandalism (War Memorial / Mungo Park).
- Reduces the likelihood of the town centre being used as a thoroughfare for criminal activity
- Reduces the likelihood of local and regional 'cruising' groups using the town centre as a racetrack
- Reduces the likelihood of criminal gangs using the local roads as a getaway between Central Scotland and North East England

SECTION 4 - OPERATION OF THE SELKIRK BIDS'S CCTV SURVEILLANCE SYSTEM

4.1. The System

4.1.1. When the system is operational images are capable of being monitored twenty-four hours a day throughout the year. All CCTV cameras are configured to record images only; any sound recording facilities will be switched off or disabled.

4.1.2. The public and community will be made aware of the presence of the system by appropriate signage which sets out the purposes for processing the CCTV images and identifies Selkirk BIDS as the Data Controller responsible for processing those images.

4.1.3. Selkirk BIDS is committed to fair, lawful, open and accountable use of CCTV. Selkirk BIDS will not use CCTV for covert monitoring except in exceptional circumstances in which all of the following conditions are met:

- that there are grounds for suspecting criminal activity or equivalent malpractice such as behaviour which puts others at risk;
- that covert monitoring is the only practical way of obtaining evidence of this malpractice;
- that informing people about the monitoring would make it difficult to prevent or detect such wrongdoing; that the camera would be used only for a specific investigation, for a specified and limited time and be removed when the investigation has been completed.

Each such use of CCTV must be authorised in advance by Selkirk BIDS Data Controller and recorded in the central log of CCTV use by the Operations Manager.

4.1.4. To ensure privacy, wherever practicable, the CCTV cameras are prevented from focusing directly or dwelling on domestic or residential accommodation. CCTV cameras located in or facing accommodation will be trained on the exterior entrances. Where it is not practicable to prevent the cameras from capturing images of such areas appropriate training will be given to system operators to ensure that they are made aware that they should not be monitoring such areas.

4.1.5. The CCTV equipment and location of each camera will be chosen to meet the quality and image capture standards necessary to achieve the Selkirk BIDS's purposes for processing the images. The location and technical specification will take account of the field of vision of the camera, light levels and other environmental conditions and minimise the capture of images that are not relevant to Selkirk BID's purposes.

In procuring and deploying CCTV equipment, Selkirk BIDS will take account of the technical standards set out by the Home Office Scientific Development Branch so that images are of sufficient quality for Selkirk BIDS's purposes. The Home Office and the Information Commissioner's Office recommend that CCTV image quality must be fit for one or more of the following purposes: .

- a) **Monitoring:** to watch the flow of traffic or the movement of people where you do not need to pick out individual figures.
- b) **Detecting:** to detect the presence of a person in the image, without needing to see their face.
- c) **Recognising:** to recognise somebody you know or determine that somebody is not known to you.
- d) **Identifying:** to record high quality facial images which can be used in court to prove someone's identity beyond reasonable doubt.

Therefore, all Selkirk BIDS CCTV images processed for the identification, apprehension, and prosecution of offenders in relation to crime and public order and for use in disciplinary investigations arising from alleged criminal activity or equivalent malpractice need to meet the quality and technical standards required for category d: identification.

CCTV equipment will be maintained and tested in accordance with a regular schedule. The Operations Manager or his nominee will be responsible for testing the quality of images to ensure that recorded images and prints as well as live images are clear and fit for purpose, taking account of seasonal variations, such as the growth of spring and summer foliage or other factors that may obscure images, and to check that date and time stamps are correct.

4.1.6. Images captured by cameras will be recorded on equipment located securely within 48 High Street, Selkirk (CCTV Operation Room). The CCTV Operation Room has monitoring equipment which allows nominated persons to monitor live images from the cameras, and any transfer of images onto other media will only take place from within the CCTV Operation Room in line with these procedures.

4.2. CCTV Operation Room

4.2.1. Images captured by the system will be monitored in the self-contained and secure CCTV Operation Room. Access to the CCTV Operation Room is strictly limited to the nominated staff members authorised by the Operations Manager. Police Officers may enter with the explicit consent

of the Operations Manager. Other persons may be authorised to enter the CCTV Operation Room on a case-by-case basis with the explicit consent of the Operations Manager with each visit being supervised at all times.

4.2.2. In an emergency, and where it is not reasonably practicable to secure prior authorisation, the nominated person may grant access to persons with a legitimate reason to enter the CCTV Operation Room. Before access is granted to any person, the nominated person must be satisfied with the identity of any visitor and the need for access.

4.2.3 Details of all visitors will be recorded in the Occurrence Log which is kept in the CCTV Operation Room.

4.2.4. The incident management system is used to record a log for each security incident including those captured on CCTV which are transferred to another medium, together with any consequential action taken.

4.2.5. Handling of images and information within the CCTV Operation Room will be carried out in accordance with these procedures and the Data Protection Act 2018. The Operations Manager will be responsible for compliance with section

SECTION 5 - MONITORING OF CCTV IMAGES

5.1. The Operations Manager and where appropriate, the nominated person will ensure that all staff (including relief/temporary staff) are fully briefed and trained in respect to all functions, both operational and administrative, arising within the operation of CCTV surveillance, including training in the data security requirements of these procedures and the Data Protection Act 2018, with input from Selkirk BIDS.

5.2. The control of the CCTV Surveillance System will always remain with Selkirk BIDS. However, at the discretion of the Secretary of Selkirk BIDS the Council may act on advice from the police in order to operate cameras during an incident to monitor potential public disorder, assist in the detection of crime or facilitate the apprehension and prosecution of offenders in relation to crime and public order. On each occasion the Police are assisted with their operations, a report setting out the time, date and detail of the incident will be submitted to the Operations Manager and the original incident will be updated within the Safeguard system.

SECTION 6 - RECORDING OF IMAGES AND RESPONDING TO ACCESS REQUESTS

6.1. Control and Management of Recordings

6.1.1. All recording media used for the monitoring and capture of images on the Selkirk BIDS CCTV system belong to and remain the property of Selkirk BIDS.

6.1.2. The CCTV Operation Room is supported by a digital recording system which stores images on appropriate media for 28 days or until capacity is reached, whichever is the shorter period, and the images are then automatically erased.

6.1.3. Should it be necessary for images to be retained for release to a third party (including the Police) under the exemptions contained within sections 28(1), 29(1)(a) and (b) and/or 35(2)(a) of the Data Protection Act 2018 or retained for any other purpose in accordance with these procedures, for which Selkirk BIDS's use of the system is registered with the Information Commissioner's Office, copies of those images will be transferred to a secure encrypted computer file.

6.1.4. Any file stored in line with 6.1.3 above shall be given a unique reference number by the person creating the file and a record made in an image tracking register contained within the CCTV Operation Room.

6.1.5. Unless required for any of the reasons contained within Section 29(3) of the Data Protection Act 1968, (2018) recorded images will be retained in the CCTV Operation Room for 28 days, after that time the images are automatically overwritten by the recording equipment.

6.1.7. Where applicable, any recording medium will be cleaned before re-use to ensure that images are not recorded on top of images previously recorded.

6.1.8. All media containing recordings will be securely destroyed at the end of their lifespans.

6.2. Access to Recordings by Staff or Third Parties

6.2.1 It is important that access to and disclosure of images is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. These aspects of these procedures reflect the second and seventh Data Protection Principles of the Data Protection Act 1998.(2018)

6.2.2. Access to recorded images will be restricted to Selkirk BIDS staff and those who require access (for instance Health & Safety Services during accident investigations or Investigating Managers in situations where serious allegations about conduct or behaviour have been made), following the consent of the Operations Manager, in order to achieve the purposes of using the equipment.

6.2.3. All requests by persons or organisations outside Selkirk BIDS (including any bodies that may claim a statutory or legal right of access) for viewing or obtaining recordings must be assessed on a case by case basis by the Operations Manager and the Data Protection Officer and the other relevant officers responsible for authorising the disclosure of persons personal data. Access will not be granted unless the responsible officers are satisfied that this is consistent with the obligations placed on Selkirk BIDS by the Data Protection Act 2018.

6.2.4. All requests for access will be recorded using Selkirk BIDS Disclosure Decision form [Appendix B] detailing:

- the date, time and purpose of the request,
- the decision to release or withhold the images and the reasons for the decision in each case,
- the date and time at which access was allowed/or disclosure made;
- the extent of the information accessed/disclosed;
- the name and role of the Data Protection officer making the decision to allow or withhold access,
- the name of the nominated person providing access.

6.2.5. The Operations Manager is responsible for documenting each request in line with section 6.2.4 above on the Safeguard incident management system. Information will be logged at the CCTV Operation Room. In all cases a copy of the record must be lodged with the responsible officers, listed in section 6.3.5 below, who maintain a complete, confidential record of all such cases on behalf of the Data Protection Officer.

6.2.6. If the Operations Manager considers that the assistance of a member of staff is needed to identify a victim, witness, or perpetrator in relation to a criminal incident, wherever practicable, the member of staff should be invited to view the images in the CCTV Operation Room.

6.3. Access by the Police

6.3.1. A police officer may request access to CCTV images held by Selkirk BIDS either by viewing such data within the CCTV Operation Room at 48 High Street, Selkirk or requesting a copy of the data. In most cases the police will request such access in response to a request by Selkirk BIDS to investigate

an alleged offence. In cases where the police request Selkirk BIDS CCTV footage to investigate an alleged offence that Selkirk BIDS has not reported, such requests for access to images are subject to the approval process set out in the Procedures for Liaison with Police.

6.3.2 During working hours, requests for CCTV footage should be referred to the Data Protection Officer

6.3.3 Outside of working hours requests for access to images should wherever possible be deferred until they can be considered by the appropriate Data Protection officer during working hours. In an emergency, if a request is straightforward and justifiable, for instance, a request for images of one incident involving criminal activity such as theft of a vehicle or equipment, the Operations Manager or nominated person may authorise disclosure to the police provided that:

- the request is in writing using the appropriate form (known as Appendix A) signed by a Senior Police Officer, who must cite the relevant exemption/s to the non-disclosure provisions of the Data Protection Act; and
- the police demonstrate that the request is proportionate and necessary for the purposes of a specific crime enquiry. In all other cases the Operations Manager or nominated person will report the request to the Data Controller to seek authorisation to take appropriate action. These procedures will be supported by underpinning guidance which will set out examples of straightforward and justifiable requests and those requiring escalation.

6.3.4. The Operations manager will complete form (see Appendix C & D) to confirm the authenticity of the recordings and arrange for all data on recordings required for disclosure to be copied onto secure encrypted media.

6.3.5. The Operations manager must complete details of the request and any disclosure made in the Incident Report in Selkirk BIDS's Safeguard electronic recording system. For each disclosure request, a copy of the completed police request form, including the reasons given for the request, together with a Selkirk BIDS Disclosure Decision form [Appendix B] recording the decision to withhold or release the information, an encrypted copy of the recording disclosed, where applicable, and reasons for the decision must be lodged with the following responsible officers who maintain a complete confidential record of all such cases on behalf of the Data Protection officer.

6.3.6. Images and recordings requested for police investigations must be supplied directly to the police, not to any third party. Requests by individuals for their own images captured on CCTV will be dealt with in accordance with the section 6.4, below.

6.3.7 The Operations Manager will liaise with the police to ensure that Selkirk BIDS is informed of the outcome of the police investigation and authorise the police to destroy any Selkirk BIDS CCTV images and recordings when they are no longer required.

6.4. Access by Data Subjects

6.4.1. Selkirk BIDS must comply with section 7 of the Data Protection Act, 2018, in informing individuals whether or not images and other information relating to them have been processed by the

CCTV Surveillance System. Individuals whose images are recorded have a right to make a request to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images. In order to comply with a request, Selkirk BIDS needs to satisfy itself as to the identity of the person making the request for their own personal data. The person making the request also needs to provide enough information to enable Selkirk BIDS staff to locate their images. Therefore, Data Subjects wishing to make a subject access request (request for data about themselves) for CCTV images / recordings / information must apply in writing to the Data Protection Officer at the address given at the end of this Procedure. In the request, the requestor must provide the following information

6.4.1.1. Dates and times of the incident or their visit to Selkirk BIDS with details of the location.

6.4.1.2. Proof of identity (e.g. driving licence/passport containing a photograph); one of these must show your current address

6.4.1.3. Payment of £20.00

6.4.1.4. Whether they require copies or view of the images in question.

6.4.2. A written decision will be sent to the data subject within **14** working days of receipt of the request. If access is agreed, such access will be provided within forty days of receipt of the request or, if later, on the date when Selkirk BIDS receives confirmation of identification from the data subject.

6.4.3. In responding to a subject access request, Selkirk BIDS staff will use red action tools to obscure images of other individuals in cases where releasing the unredacted images would involve an unfair intrusion into the privacy of the third parties concerned. Where Selkirk BIDS is unable to comply with a subject access request without disclosing information relating to another individual who can be identified from that information, it is not obliged to comply with the request unless that individual has consented to the disclosure or it is reasonable, in the circumstances, to comply without the consent of the individual.

SECTION 7 - COMPLAINTS/BREACHES

7.1. It is also recognised that other members of Selkirk BIDS or third parties may have concerns or complaints in respect to the operation of the CCTV Surveillance System. Any concerns or complaints should, in the first instance, be addressed to the Operations Manager who will follow the Selkirk BIDS Complaints Policy.

7.2. Concerns or queries relating to any aspect of compliance with the Data Protection Act, 1998, (2018) should be directed to the Data Protection Officer.

SECTION 8 - RESPONSIBLE OFFICER

The Operations Manager is responsible for the implementation of these procedures, in consultation with the Data Protection Officer.

SECTION 9 - MONITORING AND REVIEW

The Operations Manager and the Data Protection Officer will monitor compliance with these procedures and the operational effectiveness of the Selkirk BIDS CCTV systems, reporting to the Information Governance and Security Group. These officers will initiate reviews of the procedure out with the annual review cycle where necessary in the light of developments in the current legislation which underpins the procedures. Selkirk BIDS Information Governance and Security Group will review these procedures annually. The review will consider the effectiveness of the procedures and will take account of the views of stakeholders and relevant developments relating to the Data Protection Act, the statutory CCTV Code of Practice and other relevant legislation. Following review, these procedures will be revised and updated as appropriate.



SECTION 10 - RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

Information Security Policy Framework

SELKIRK BIDS

CCTV PROCEDURES – To support Information Security Policy Framework

CCTV Codes of Practice

SELKIRK BIDS

Code of Practice - Public Space CCTV

Data Protection Policy and Guidance

SELKIRK BIDS

PRIVACY NOTICE

SECTION 11 - FURTHER HELP AND ADVICE

For more information and advice about these procedures contact

Data Protection Officer

SELKIRK BIDS

48 High Street

SELKIRK

TD7 4DD

Email: davcanderson@aol.com

Web: <https://www.exploreselkirk.co.uk>



SELKIRK BIDS

PROCEDURES – To support Information Security Policy Framework 30/01/2023

SUBJECT ACCESS REQUEST FORM APPENDIX C

Selkirk BIDS – CCTV

DATA PROTECTION ACT 2018 (incorporating GDPR 2018)

How to Apply For Access To Information Held On the SELKIRK BIDS – CCTV System

These notes explain how you can find out what information, if any, is held about you on the CCTV System. Please note that CCTV images are only retained for 28 days.

Your Rights

Subject to certain exemptions, you have a right to be told whether any personal data is held about you. You also have a right to a copy of that information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or if you agree otherwise. NDCC Council will only give that information if it is satisfied as to your identity. If release of the information will disclose information relating to another individual(s), who can be identified from that information, the Council is not obliged to comply with an access request unless –

- The other individual has consented to the disclosure of information, or
- It is reasonable in all the circumstances to comply with the request without the consent of the other individual(s)

SELKIRK BIDS's Rights

Selkirk BIDS may deny access to information where the Regulation allows. The main exemptions in relation to information held on the CCTV System are where the information may be held for: Prevention and detection of crime

- Apprehension and prosecution of offenders
- And giving you the information may be likely to prejudice any of these purposes.

Fee

A fee to deal with this request is £20.00 in most circumstances. Applications can be made using this form

The Application Form: all sections of the form must be completed.

Section 1 Asks you to give information about yourself that will help confirm your identity. Selkirk BIDS has a duty to ensure that information it holds is secure and it must be satisfied that you are who you say you are.

Section 2 Asks you to provide evidence of your identity TWO pieces of ID (e.g. driving licence/passport containing a photograph); one of these must show your current address

Section 3 Asks you to confirm whether you will accept just viewing the information, or if you want a copy of the information.

Section 4 You must sign the declaration



SELKIRK BIDS

COMMUNITY PROCEDURES – To support Information Security Policy Framework 30/01/2023
COUNCIL

SUBJECT ACCESS REQUEST FORM APPENDIX D

SELKIRK BIDS CCTV SURVEILLANCE SYSTEM

DATA PROTECTION ACT 2018 (incorporating the GDPR 2018)

SECTION 1 About Yourself

The information requested below is to help NDCC satisfy itself as to your identity and find any data requested

PLEASE USE BLOCK LETTERS

Title (tick box as appropriate) Mr Mrs Miss Ms

Other title (e.g. Dr., Rev., etc.)

Surname/family name

First names

Maiden name/former names

Your Current Home Address

Post Code

A telephone number will be helpful in case you need to be contacted.

Tel. No.

SECTION 2 Proof of Identity

To establish your identity your application must be accompanied by TWO pieces of ID (e.g. driving licence/passport containing a photograph); one of these must show your current address

SECTION 3 Supply of Information

You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form. Do you wish to:

(a) View the information and receive a permanent copy YES/NO

(b) Only view the information YES/NO

SECTION 4 Declaration

DECLARATION (to be signed by the applicant)

The information that I have supplied in this application is correct and I am the person to whom it relates.

Signed by _____

Date ____/____/____

Warning – a person who impersonates or attempts to impersonate another may be guilty of an offence.

This page is intentionally left blank

**PROCEDURES FOR OPERATION OF CCTV ON NEWCASTLETON DISTRICT COMMUNITY COUNCIL
(NDCC) PREMISES TO SUPPORT INFORMATION SECURITY POLICY FRAMEWORK**

CONTENTS

1 INTRODUCTION

2 SCOPE

3 OBJECTIVES

4 OPERATION OF THE NDCC'S CCTV SURVEILLANCE SYSTEM

5 MONITORING OF CCTV IMAGES

6 RECORDING OF IMAGES AND RESPONDING TO ACCESS REQUESTS

7 COMPLAINTS/BREACHES

8 RESPONSIBLE OFFICER

9 MONITORING AND REVIEW

10 RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

11 FURTHER HELP AND ADVICE

Appendix A - Access documents

SECTION 1 - INTRODUCTION

These procedures are applicable to all NDCC staff or their nominated representatives. Their purpose is to ensure that the NDCC Closed Circuit Television (CCTV) system is used to create a safer environment for residents, and visitors to Newcastleton and to ensure that its operation is consistent with the obligations on the NDCC imposed by the Data Protection Act 2018.

For the purposes of the Data Protection Act 2018, the Data Controller is NDCC. The NDCC has installed a comprehensive CCTV surveillance system across Newcastleton for the principal purposes of flood protection monitoring, together with preventing and detecting crime and promoting public safety.

The images from the CCTV system are located in Buccleuch House (CCTV Operation Room).

It is recognised that ancillary benefits of operating CCTV for this purpose may include reduction of the fear of crime generally and the provision of a safer public environment for the benefit of those who live or work within and visit the village.

CCTV Cameras which are located on buildings are the responsibility of the NDCC who is accountable for compliance with these procedures. Following the introduction of these procedures a programme will be agreed to manage the migration of all NDCC CCTV cameras onto a common platform which will allow all recordings to be monitored from the Buccleuch House.

Due to public concern surrounding a surveillance society, the use of CCTV surveillance must be consistent with respect for individuals' privacy. Other methods of achieving the objectives of a CCTV surveillance system will therefore be considered before installation of any CCTV camera positions.

SECTION 2 - SCOPE

These procedures apply to all NDCC CCTV cameras and equipment across Newcastleton. The NDCC is the Data Controller for this system, determines the purpose of recording and is legally responsible and accountable for its use. These procedures will be adapted to apply to all systems for which the NDCC is the Data Controller for all camera locations.

SECTION 3 - OBJECTIVES

The NDCC CCTV surveillance system has been installed and is monitored for the following purposes:

- Provides a series of linked cameras for all entrances to our village as well as capture locations prone to regular vandalism (school, Polysport, riverside).
- Reduces the likelihood of the village being used as a thoroughfare for criminal activity
- Reduces the likelihood of local and regional 'cruising' groups using the village as a racetrack
- Reduces the likelihood of criminal gangs using the forest roads as a getaway between Central Scotland and North East England.
- Provides 'remote live views' for our resilience team and SBC Emergency bunker to see real time events on the river Liddel.
- Captures footage over time to help understand changing river behaviours, using the findings to refine the flood scheme.
- Provides a 20-minute warning to residents to try to avoid the devastation Storm Dennis caused in Feb 2020 with a further flood event in Feb 2021 causing substantial damage within the community.

SECTION 4 - OPERATION OF THE NDCC'S CCTV SURVEILLANCE SYSTEM

4.1. The System

4.1.1. When the system is operational images are capable of being monitored twenty-four hours a day throughout the year. All CCTV cameras are configured to record images only: any sound recording facilities will be switched off or disabled.

4.1.2. The public and community will be made aware of the presence of the system by appropriate signage which sets out the purposes for processing the CCTV images and identifies the NDCC as the Data Controller responsible for processing those images.

4.1.3. The NDCC is committed to fair, lawful, open and accountable use of CCTV. The NDCC will not use CCTV for covert monitoring except in exceptional circumstances in which all of the following conditions are met:

- that there are grounds for suspecting criminal activity or equivalent malpractice such as behaviour which puts others at risk;
- that covert monitoring is the only practical way of obtaining evidence of this malpractice;
- that informing people about the monitoring would make it difficult to prevent or detect such wrongdoing; that the camera would be used only for a specific investigation, for a specified and limited time and be removed when the investigation has been completed.

Each such use of CCTV must be authorised in advance by the NDCC Data Controller and recorded in the central log of CCTV use by the Operations Manager.

4.1.4. To ensure privacy, wherever practicable, the CCTV cameras are prevented from focusing directly or dwelling on domestic or residential accommodation. CCTV cameras located in or facing accommodation will be trained on the exterior entrances. Where it is not practicable to prevent the cameras from capturing images of such areas appropriate training will be given to system operators to ensure that they are made aware that they should not be monitoring such areas.

4.1.5. The CCTV equipment and location of each camera will be chosen to meet the quality and image capture standards necessary to achieve the NDCC's purposes for processing the images. The location and technical specification will take account of the field of vision of the camera, light levels and other environmental conditions and minimise the capture of images that are not relevant to the NDCC's purposes.

In procuring and deploying CCTV equipment, the NDCC will take account of the technical standards set out by the Home Office Scientific Development Branch so that images are of sufficient quality for the NDCC's purposes. The Home Office and the Information Commissioner's Office recommend that CCTV image quality must be fit for one or more of the following purposes: .

- a) **Monitoring:** to watch the flow of traffic or the movement of people where you do not need to pick out individual figures.
- b) **Detecting:** to detect the presence of a person in the image, without needing to see their face.

- c) Recognising: to recognise somebody you know or determine that somebody is not known to you.
- d) Identifying: to record high quality facial images which can be used in court to prove someone's identity beyond reasonable doubt.

Therefore, all NDCC CCTV images processed for the identification, apprehension, and prosecution of offenders in relation to crime and public order and for use in disciplinary investigations arising from alleged criminal activity or equivalent malpractice need to meet the quality and technical standards required for category d: identification.

CCTV equipment will be maintained and tested in accordance with a regular schedule. The Operations Manager or his nominee will be responsible for testing the quality of images to ensure that recorded images and prints as well as live images are clear and fit for purpose, taking account of seasonal variations, such as the growth of spring and summer foliage or other factors that may obscure images, and to check that date and time stamps are correct.

4.1.6. Images captured by cameras will be recorded on equipment located securely within Buccleuch House (CCTV Operation Room). The CCTV Operation Room has monitoring equipment which allows nominated persons to monitor live images from the cameras, and any transfer of images onto other media will only take place from within the CCTV Operation Room in line with these procedures.

4.2. CCTV Operation Room

4.2.1. Images captured by the system will be monitored in the self-contained and secure CCTV Operation Room. Access to the CCTV Operation Room is strictly limited to the nominated staff members authorised by the Operations Manager. Police Officers may enter with the explicit consent of the Operations Manager. Other persons may be authorised to enter the CCTV Operation Room on a case-by-case basis with the explicit consent of the Operations Manager with each visit being supervised at all times.

4.2.2. In an emergency, and where it is not reasonably practicable to secure prior authorisation, the nominated person may grant access to persons with a legitimate reason to enter the CCTV Operation Room. Before access is granted to any person, the nominated person must be satisfied with the identity of any visitor and the need for access.

4.2.3 Details of all visitors will be recorded in the Occurrence Log which is kept in the CCTV Operation Room.

4.2.4. The incident management system is used to record a log for each security incident including those captured on CCTV which are transferred to another medium, together with any consequential action taken.

4.2.5. Handling of images and information within the CCTV Operation Room will be carried out in accordance with these procedures and the Data Protection Act 2018. The Operations Manager will be responsible for compliance with section

SECTION 5 - MONITORING OF CCTV IMAGES

5.1. The Operations Manager and where appropriate, the nominated person will ensure that all staff (including relief/temporary staff) are fully briefed and trained in respect to all functions, both operational and administrative, arising within the operation of CCTV surveillance, including training in the data security requirements of these procedures and the Data Protection Act 2018, with input from the NDCC.

5.2. The control of the CCTV Surveillance System will always remain with the NDCC. However, at the discretion of the Secretary of the NDCC the Council may act on advice from the police in order to operate cameras during an incident to monitor potential public disorder, assist in the detection of crime or facilitate the apprehension and prosecution of offenders in relation to crime and public order. On each occasion the Police are assisted with their operations, a report setting out the time, date and detail of the incident will be submitted to the Operations Manager and the original incident will be updated within the Safeguard system.

SECTION 6 - RECORDING OF IMAGES AND RESPONDING TO ACCESS REQUESTS

6.1. Control and Management of Recordings

6.1.1. All recording media used for the monitoring and capture of images on the NDCC CCTV system belong to and remain the property of the NDCC.

6.1.2. The CCTV Operation Room is supported by a digital recording system which stores images on appropriate media for 28 days or until capacity is reached, whichever is the shorter period, and the images are then automatically erased.

6.1.3. Should it be necessary for images to be retained for release to a third party (including the Police) under the exemptions contained within sections 28(1), 29(1)(a) and (b) and/or 35(2)(a) of the Data Protection Act 2018 or retained for any other purpose in accordance with these procedures, for which the NDCC's use of the system is registered with the Information Commissioner's Office, copies of those images will be transferred to a secure encrypted computer file.

6.1.4. Any file stored in line with 6.1.3 above shall be given a unique reference number by the person creating the file and a record made in an image tracking register contained within the CCTV Operation Room.

6.1.5. Unless required for any of the reasons contained within Section 29(3) of the Data Protection Act 1968, (2018) recorded images will be retained in the CCTV Operation Room for 28 days, after that time the images are automatically overwritten by the recording equipment. Flood management images will be retained for a period of 90 days.

6.1.7. Where applicable, any recording medium will be cleaned before re-use to ensure that images are not recorded on top of images previously recorded.

6.1.8. All media containing recordings will be securely destroyed at the end of their lifespans.

6.2. Access to Recordings by Staff or Third Parties

6.2.1 It is important that access to and disclosure of images is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. These aspects of these procedures reflect the second and seventh Data Protection Principles of the Data Protection Act 1998.(2018)

6.2.2. Access to recorded images will be restricted to NDCC staff and those who require access (for instance Health & Safety Services during accident investigations or Investigating Managers in situations where serious allegations about conduct or behaviour have been made), following the consent of the Operations Manager, in order to achieve the purposes of using the equipment.

6.2.3. All requests by persons or organisations outside the NDCC(including any bodies that may claim a statutory or legal right of access) for viewing or obtaining recordings must be assessed on a case by case basis by the Operations Manager and the Data Protection Officer and the other relevant officers responsible for authorising the disclosure of persons personal data. Access will not be granted unless the responsible officers are satisfied that this is consistent with the obligations placed on the NDCC by the Data Protection Act 2018.

6.2.4. All requests for access will be recorded using the NDCC Disclosure Decision form [Appendix B] detailing:

- the date, time and purpose of the request,
- the decision to release or withhold the images and the reasons for the decision in each case,
- the date and time at which access was allowed/or disclosure made;
- the extent of the information accessed/disclosed;
- the name and role of the Data Protection officer making the decision to allow or withhold access,
- the name of the nominated person providing access.

6.2.5. The Operations Manager is responsible for documenting each request in line with section 6.2.4 above on the Safeguard incident management system. Information will be logged at the CCTV Operation Room. In all cases a copy of the record must be lodged with the responsible officers, listed in section 6.3.5 below, who maintain a complete, confidential record of all such cases on behalf of the Data Protection Officer.

6.2.6. If the Operations Manager considers that the assistance of a member of staff is needed to identify a victim, witness, or perpetrator in relation to a criminal incident, wherever practicable, the member of staff should be invited to view the images in the CCTV Operation Room.

6.3. Access by the Police

6.3.1. A police officer may request access to CCTV images held by the NDCC either by viewing such data within the CCTV Operation Room at Buccleuch House or requesting a copy of the data. In most cases the police will request such access in response to a request by the NDCC to investigate an alleged

offence. In cases where the police request NDCC CCTV footage to investigate an alleged offence that the NDCC has not reported, such requests for access to images are subject to the approval process set out in the Procedures for Liaison with Police.

6.3.2 During working hours, requests for CCTV footage should be referred to the Data Protection Officer

6.3.3 Outside of working hours requests for access to images should wherever possible be deferred until they can be considered by the appropriate Data Protection officer during working hours. In an emergency, if a request is straightforward and justifiable, for instance, a request for images of one incident involving criminal activity such as theft of a vehicle or equipment, the Operations Manager or nominated person may authorise disclosure to the police provided that:

- the request is in writing using the appropriate form (known as Appendix A) signed by a Senior Police Officer, who must cite the relevant exemption/s to the non-disclosure provisions of the Data Protection Act; and
- the police demonstrate that the request is proportionate and necessary for the purposes of a specific crime enquiry. In all other cases the Operations Manager or nominated person will report the request to the Data Controller to seek authorisation to take appropriate action. These procedures will be supported by underpinning guidance which will set out examples of straightforward and justifiable requests and those requiring escalation.

6.3.4. The Operations manager will complete form (see Appendix C & D) to confirm the authenticity of the recordings and arrange for all data on recordings required for disclosure to be copied onto secure encrypted media.

6.3.5. The Operations manager must complete details of the request and any disclosure made in the Incident Report in the NDCC's Safeguard electronic recording system. For each disclosure request, a copy of the completed police request form, including the reasons given for the request, together with a NDCC Disclosure Decision form [Appendix B] recording the decision to withhold or release the information, an encrypted copy of the recording disclosed, where applicable, and reasons for the decision must be lodged with the following responsible officers who maintain a complete confidential record of all such cases on behalf of the Data Protection officer.

6.3.6. Images and recordings requested for police investigations must be supplied directly to the police, not to any third party. Requests by individuals for their own images captured on CCTV will be dealt with in accordance with the section 6.4, below.

6.3.7 The Operations Manager will liaise with the police to ensure that the NDCC is informed of the outcome of the police investigation and authorise the police to destroy any NDCC CCTV images and recordings when they are no longer required.

6.4. Access by Data Subjects

6.4.1. The NDCC must comply with section 7 of the Data Protection Act, 2018, in informing individuals whether or not images and other information relating to them have been processed by the CCTV

Surveillance System. Individuals whose images are recorded have a right to make a request to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images. In order to comply with a request, the NDCC needs to satisfy itself as to the identity of the person making the request for their own personal data. The person making the request also needs to provide enough information to enable NDCC staff to locate their images. Therefore, Data Subjects wishing to make a subject access request (request for data about themselves) for CCTV images / recordings / information must apply in writing to the Data Protection Officer at the address given at the end of this Procedure. In the request, the requestor must provide the following information

6.4.1.1. Dates and times of the incident or their visit to the NDCC with details of the location.

6.4.1.2. Proof of identity (e.g. driving licence/passport containing a photograph); one of these must show your current address

6.4.1.3. Payment of £0.00

6.4.1.4. Whether they require copies or view of the images in question.

6.4.2. A written decision will be sent to the data subject within **14** working days of receipt of the request. If access is agreed, such access will be provided within forty days of receipt of the request or, if later, on the date when the NDCC receives confirmation of identification from the data subject.

6.4.3. In responding to a subject access request, NDCC staff will use red action tools to obscure images of other individuals in cases where releasing the unredacted images would involve an unfair intrusion into the privacy of the third parties concerned. Where the NDCC is unable to comply with a subject access request without disclosing information relating to another individual who can be identified from that information, it is not obliged to comply with the request unless that individual has consented to the disclosure or it is reasonable, in the circumstances, to comply without the consent of the individual.

SECTION 7 - COMPLAINTS/BREACHES

7.1. It is also recognised that other members of the NDCC or third parties may have concerns or complaints in respect to the operation of the CCTV Surveillance System. Any concerns or complaints should, in the first instance, be addressed to the Operations Manager who will follow the NDCC Complaints Policy.

7.2. Concerns or queries relating to any aspect of compliance with the Data Protection Act, 1998, (2018) should be directed to the Data Protection Officer.

SECTION 8 - RESPONSIBLE OFFICER

The Operations Manager is responsible for the implementation of these procedures, in consultation with the Data Protection Officer.

SECTION 9 - MONITORING AND REVIEW

The Operations Manager and the Data Protection Officer will monitor compliance with these procedures and the operational effectiveness of the NDCC CCTV systems, reporting to the Information Governance and Security Group. These officers will initiate reviews of the procedure out with the annual review cycle where necessary in the light of developments in the current legislation which underpins the procedures. The NDCC Information Governance and Security Group will review these procedures annually. The review will consider the effectiveness of the procedures and will take account of the views of stakeholders and relevant developments relating to the Data Protection Act, the statutory CCTV Code of Practice and other relevant legislation. Following review, these procedures will be revised and updated as appropriate.

SECTION 10 - RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

Information Security Policy Framework
NEWCASTLETON DISTRICT COMMUNITY COUNCIL
CCTV PROCEDURES – To support Information Security Policy Framework

CCTV Codes of Practice
NEWCASTLETON DISTRICT COMMUNITY COUNCIL
Code of Practice - Public Space CCTV

Data Protection Policy and Guidance
NEWCASTLETON DISTRICT COMMUNITY COUNCIL
PRIVACY NOTICE

SECTION 11 - FURTHER HELP AND ADVICE

For more information and advice about these procedures contact
Data Protection Officer
Newcastleton District Community Council
4 South Hermitage Street
NEWCASTLETON
TD9 0QR
Email: secretary@newcastletoncommunitytrust.co.uk
Web: <https://www.visitnewcastleton.com/>

SUBJECT ACCESS REQUEST FORM APPENDIX C

**NEWCASTLETON DISTRICT COMMUNITY COUNCIL (NDCC) – CCTV
 DATA PROTECTION ACT 2018 (incorporating GDPR 2018)**

How to Apply For Access To Information Held On the Newcastleton District Community Council – CCTV System
 These notes explain how you can find out what information, if any, is held about you on the CCTV System. Please note that CCTV images are only retained for 28 days.

Your Rights

Subject to certain exemptions, you have a right to be told whether any personal data is held about you. You also have a right to a copy of that information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or if you agree otherwise. NDCC Council will only give that information if it is satisfied as to your identity. If release of the information will disclose information relating to another individual(s), who can be identified from that information, the Council is not obliged to comply with an access request unless –

- The other individual has consented to the disclosure of information, or
- It is reasonable in all the circumstances to comply with the request without the consent of the other individual(s)

NDCC Council's Rights

NDCC Council may deny access to information where the Regulation allows. The main exemptions in relation to information held on the CCTV System are where the information may be held for: Prevention and detection of crime

- Apprehension and prosecution of offenders
- And giving you the information may be likely to prejudice any of these purposes.

Fee

A fee to deal with this request is £0.00 in most circumstances. Applications can be made using this form

The Application Form: all sections of the form must be completed.

Section 1 Asks you to give information about yourself that will help confirm your identity. NDCC has a duty to ensure that information it holds is secure and it must be satisfied that you are who you say you are.

Section 2 Asks you to provide evidence of your identity TWO pieces of ID (e.g. driving licence/passport containing a photograph); one of these must show your current address

Section 3 Asks you to confirm whether you will accept just viewing the information, or if you want a copy of the information.

Section 4 You must sign the declaration

SUBJECT ACCESS REQUEST FORM APPENDIX D				
NDCC CCTV SURVEILLANCE SYSTEM				
DATA PROTECTION ACT 2018 (incorporating the GDPR 2018)				
SECTION 1 About Yourself				
The information requested below is to help NDCC satisfy itself as to your identity and find any data requested				
PLEASE USE BLOCK LETTERS				
Title (tick box as appropriate)	Mr	Mrs	Miss	Ms
Other title (e.g. Dr., Rev., etc.)				
Surname/family name				
First names				
Maiden name/former names				
Your Current Home Address				
Post Code				
A telephone number will be helpful in case you need to be contacted. Tel. No.				
SECTION 2 Proof of Identity				
To establish your identity your application must be accompanied by TWO pieces of ID (e.g. driving licence/passport containing a photograph); one of these must show your current address				
SECTION 3 Supply of Information				
You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form. Do you wish to:				
(a) View the information and receive a permanent copy	YES/NO			
(b) Only view the information	YES/NO			
SECTION 4 Declaration				
DECLARATION (to be signed by the applicant)				
The information that I have supplied in this application is correct and I am the person to whom it relates.				
Signed by _____				
Date ____/____/____				
Warning – a person who impersonates or attempts to impersonate another may be guilty of an offence.				

This page is intentionally left blank

SELKIRK BIDS

CCTV PROCEDURES – To support Information Security Policy Framework 30/01/2023

PROCEDURES FOR OPERATION OF CCTV ON SELKIRK BIDS PREMISES TO SUPPORT INFORMATION SECURITY POLICY FRAMEWORK

CONTENTS

1 INTRODUCTION

2 SCOPE

3 OBJECTIVES

4 OPERATION OF THE NDCC'S CCTV SURVEILLANCE SYSTEM

5 MONITORING OF CCTV IMAGES

6 RECORDING OF IMAGES AND RESPONDING TO ACCESS REQUESTS

7 COMPLAINTS/BREACHES

8 RESPONSIBLE OFFICER

9 MONITORING AND REVIEW

10 RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

11 FURTHER HELP AND ADVICE

Appendix A - Access documents

SELKIRK BIDS

CCTV PROCEDURES – To support Information Security Policy Framework 30/01/2023

SECTION 1 - INTRODUCTION

These procedures are applicable to all Selkirk BIDS staff or their nominated representatives. Their purpose is to ensure that the Selkirk BIDS Closed Circuit Television (CCTV) system is used to create a safer environment for residents, and visitors to Selkirk and to ensure that its operation is consistent with the obligations on Selkirk BIDS imposed by the Data Protection Act 2018.

For the purposes of the Data Protection Act 2018, the Data Controller is Selkirk BIDS. Selkirk BIDS has installed a comprehensive CCTV surveillance system across Selkirk for the principal purposes of preventing and detecting crime and promoting public safety.

The images from the CCTV system are located in 48 High Street, Selkirk (CCTV Operation Room).

It is recognised that ancillary benefits of operating CCTV for this purpose may include reduction of the fear of crime generally and the provision of a safer public environment for the benefit of those who live or work within and visit the town.

CCTV Cameras which are located on buildings are the responsibility of Selkirk BIDS who is accountable for compliance with these procedures. Following the introduction of these procedures a programme will be agreed to manage the migration of all Selkirk BIDS CCTV cameras onto a common platform which will allow all recordings to be monitored from 48 High Street, Selkirk.

Due to public concern surrounding a surveillance society, the use of CCTV surveillance must be consistent with respect for individuals' privacy. Other methods of achieving the objectives of a CCTV surveillance system will therefore be considered before installation of any CCTV camera positions.

SELKIRK BIDS

CCTV PROCEDURES – To support Information Security Policy Framework 30/01/2023

SECTION 2 - SCOPE

These procedures apply to all Selkirk BIDS CCTV cameras and equipment across Selkirk. Selkirk BIDS is the Data Controller for this system, determines the purpose of recording and is legally responsible and accountable for its use. These procedures will be adapted to apply to all systems for which Selkirk BIDS is the Data Controller for all camera locations.

SECTION 3 - OBJECTIVES

Selkirk BIDS CCTV surveillance system has been installed and is monitored for the following purposes:

- Provides a series of linked cameras for all entrances to our town centre as well as capture locations prone to regular vandalism (War Memorial / Mungo Park).
- Reduces the likelihood of the town centre being used as a thoroughfare for criminal activity
- Reduces the likelihood of local and regional 'cruising' groups using the town centre as a racetrack
- Reduces the likelihood of criminal gangs using the local roads as a getaway between Central Scotland and North East England

SECTION 4 - OPERATION OF THE SELKIRK BIDS'S CCTV SURVEILLANCE SYSTEM

4.1. The System

4.1.1. When the system is operational images are capable of being monitored twenty-four hours a day throughout the year. All CCTV cameras are configured to record images only; any sound recording facilities will be switched off or disabled.

4.1.2. The public and community will be made aware of the presence of the system by appropriate signage which sets out the purposes for processing the CCTV images and identifies Selkirk BIDS as the Data Controller responsible for processing those images.

4.1.3. Selkirk BIDS is committed to fair, lawful, open and accountable use of CCTV. Selkirk BIDS will not use CCTV for covert monitoring except in exceptional circumstances in which all of the following conditions are met:

- that there are grounds for suspecting criminal activity or equivalent malpractice such as behaviour which puts others at risk;
- that covert monitoring is the only practical way of obtaining evidence of this malpractice;
- that informing people about the monitoring would make it difficult to prevent or detect such wrongdoing; that the camera would be used only for a specific investigation, for a specified and limited time and be removed when the investigation has been completed.

Each such use of CCTV must be authorised in advance by Selkirk BIDS Data Controller and recorded in the central log of CCTV use by the Operations Manager.

SELKIRK BIDS

CCTV PROCEDURES – To support Information Security Policy Framework 30/01/2023

4.1.4. To ensure privacy, wherever practicable, the CCTV cameras are prevented from focusing directly or dwelling on domestic or residential accommodation. CCTV cameras located in or facing accommodation will be trained on the exterior entrances. Where it is not practicable to prevent the cameras from capturing images of such areas appropriate training will be given to system operators to ensure that they are made aware that they should not be monitoring such areas.

4.1.5. The CCTV equipment and location of each camera will be chosen to meet the quality and image capture standards necessary to achieve the Selkirk BIDS's purposes for processing the images. The location and technical specification will take account of the field of vision of the camera, light levels and other environmental conditions and minimise the capture of images that are not relevant to Selkirk BID's purposes.

In procuring and deploying CCTV equipment, Selkirk BIDS will take account of the technical standards set out by the Home Office Scientific Development Branch so that images are of sufficient quality for Selkirk BIDS's purposes. The Home Office and the Information Commissioner's Office recommend that CCTV image quality must be fit for one or more of the following purposes: .

- a) **Monitoring:** to watch the flow of traffic or the movement of people where you do not need to pick out individual figures.
- b) **Detecting:** to detect the presence of a person in the image, without needing to see their face.
- c) **Recognising:** to recognise somebody you know or determine that somebody is not known to you.
- d) **Identifying:** to record high quality facial images which can be used in court to prove someone's identity beyond reasonable doubt.

Therefore, all Selkirk BIDS CCTV images processed for the identification, apprehension, and prosecution of offenders in relation to crime and public order and for use in disciplinary investigations arising from alleged criminal activity or equivalent malpractice need to meet the quality and technical standards required for category d: identification.

CCTV equipment will be maintained and tested in accordance with a regular schedule. The Operations Manager or his nominee will be responsible for testing the quality of images to ensure that recorded images and prints as well as live images are clear and fit for purpose, taking account of seasonal variations, such as the growth of spring and summer foliage or other factors that may obscure images, and to check that date and time stamps are correct.

4.1.6. Images captured by cameras will be recorded on equipment located securely within 48 High Street, Selkirk (CCTV Operation Room). The CCTV Operation Room has monitoring equipment which allows nominated persons to monitor live images from the cameras, and any transfer of images onto other media will only take place from within the CCTV Operation Room in line with these procedures.

4.2. CCTV Operation Room

4.2.1. Images captured by the system will be monitored in the self-contained and secure CCTV Operation Room. Access to the CCTV Operation Room is strictly limited to the nominated staff members authorised by the Operations Manager. Police Officers may enter with the explicit consent

SELKIRK BIDS

CCTV PROCEDURES – To support Information Security Policy Framework 30/01/2023

of the Operations Manager. Other persons may be authorised to enter the CCTV Operation Room on a case-by-case basis with the explicit consent of the Operations Manager with each visit being supervised at all times.

4.2.2. In an emergency, and where it is not reasonably practicable to secure prior authorisation, the nominated person may grant access to persons with a legitimate reason to enter the CCTV Operation Room. Before access is granted to any person, the nominated person must be satisfied with the identity of any visitor and the need for access.

4.2.3 Details of all visitors will be recorded in the Occurrence Log which is kept in the CCTV Operation Room.

4.2.4. The incident management system is used to record a log for each security incident including those captured on CCTV which are transferred to another medium, together with any consequential action taken.

4.2.5. Handling of images and information within the CCTV Operation Room will be carried out in accordance with these procedures and the Data Protection Act 2018. The Operations Manager will be responsible for compliance with section

SELKIRK BIDS

CCTV PROCEDURES – To support Information Security Policy Framework 30/01/2023

SECTION 5 - MONITORING OF CCTV IMAGES

5.1. The Operations Manager and where appropriate, the nominated person will ensure that all staff (including relief/temporary staff) are fully briefed and trained in respect to all functions, both operational and administrative, arising within the operation of CCTV surveillance, including training in the data security requirements of these procedures and the Data Protection Act 2018, with input from Selkirk BIDS.

5.2. The control of the CCTV Surveillance System will always remain with Selkirk BIDS. However, at the discretion of the Secretary of Selkirk BIDS the Council may act on advice from the police in order to operate cameras during an incident to monitor potential public disorder, assist in the detection of crime or facilitate the apprehension and prosecution of offenders in relation to crime and public order. On each occasion the Police are assisted with their operations, a report setting out the time, date and detail of the incident will be submitted to the Operations Manager and the original incident will be updated within the Safeguard system.

SECTION 6 - RECORDING OF IMAGES AND RESPONDING TO ACCESS REQUESTS

6.1. Control and Management of Recordings

6.1.1. All recording media used for the monitoring and capture of images on the Selkirk BIDS CCTV system belong to and remain the property of Selkirk BIDS.

6.1.2. The CCTV Operation Room is supported by a digital recording system which stores images on appropriate media for 28 days or until capacity is reached, whichever is the shorter period, and the images are then automatically erased.

6.1.3. Should it be necessary for images to be retained for release to a third party (including the Police) under the exemptions contained within sections 28(1), 29(1)(a) and (b) and/or 35(2)(a) of the Data Protection Act 2018 or retained for any other purpose in accordance with these procedures, for which Selkirk BIDS's use of the system is registered with the Information Commissioner's Office, copies of those images will be transferred to a secure encrypted computer file.

6.1.4. Any file stored in line with 6.1.3 above shall be given a unique reference number by the person creating the file and a record made in an image tracking register contained within the CCTV Operation Room.

6.1.5. Unless required for any of the reasons contained within Section 29(3) of the Data Protection Act 1968, (2018) recorded images will be retained in the CCTV Operation Room for 28 days, after that time the images are automatically overwritten by the recording equipment.

6.1.7. Where applicable, any recording medium will be cleaned before re-use to ensure that images are not recorded on top of images previously recorded.

6.1.8. All media containing recordings will be securely destroyed at the end of their lifespans.

SELKIRK BIDS

CCTV PROCEDURES – To support Information Security Policy Framework 30/01/2023

6.2. Access to Recordings by Staff or Third Parties

6.2.1 It is important that access to and disclosure of images is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. These aspects of these procedures reflect the second and seventh Data Protection Principles of the Data Protection Act 1998.(2018)

6.2.2. Access to recorded images will be restricted to Selkirk BIDS staff and those who require access (for instance Health & Safety Services during accident investigations or Investigating Managers in situations where serious allegations about conduct or behaviour have been made), following the consent of the Operations Manager, in order to achieve the purposes of using the equipment.

6.2.3. All requests by persons or organisations outside Selkirk BIDS (including any bodies that may claim a statutory or legal right of access) for viewing or obtaining recordings must be assessed on a case by case basis by the Operations Manager and the Data Protection Officer and the other relevant officers responsible for authorising the disclosure of persons personal data. Access will not be granted unless the responsible officers are satisfied that this is consistent with the obligations placed on Selkirk BIDS by the Data Protection Act 2018.

6.2.4. All requests for access will be recorded using Selkirk BIDS Disclosure Decision form [Appendix B] detailing:

- the date, time and purpose of the request,
- the decision to release or withhold the images and the reasons for the decision in each case,
- the date and time at which access was allowed/or disclosure made;
- the extent of the information accessed/disclosed;
- the name and role of the Data Protection officer making the decision to allow or withhold access,
- the name of the nominated person providing access.

6.2.5. The Operations Manager is responsible for documenting each request in line with section 6.2.4 above on the Safeguard incident management system. Information will be logged at the CCTV Operation Room. In all cases a copy of the record must be lodged with the responsible officers, listed in section 6.3.5 below, who maintain a complete, confidential record of all such cases on behalf of the Data Protection Officer.

6.2.6. If the Operations Manager considers that the assistance of a member of staff is needed to identify a victim, witness, or perpetrator in relation to a criminal incident, wherever practicable, the member of staff should be invited to view the images in the CCTV Operation Room.

6.3. Access by the Police

6.3.1. A police officer may request access to CCTV images held by Selkirk BIDS either by viewing such data within the CCTV Operation Room at 48 High Street, Selkirk or requesting a copy of the data. In most cases the police will request such access in response to a request by Selkirk BIDS to investigate

SELKIRK BIDS

CCTV PROCEDURES – To support Information Security Policy Framework 30/01/2023

an alleged offence. In cases where the police request Selkirk BIDS CCTV footage to investigate an alleged offence that Selkirk BIDS has not reported, such requests for access to images are subject to the approval process set out in the Procedures for Liaison with Police.

6.3.2 During working hours, requests for CCTV footage should be referred to the Data Protection Officer

6.3.3 Outside of working hours requests for access to images should wherever possible be deferred until they can be considered by the appropriate Data Protection officer during working hours. In an emergency, if a request is straightforward and justifiable, for instance, a request for images of one incident involving criminal activity such as theft of a vehicle or equipment, the Operations Manager or nominated person may authorise disclosure to the police provided that:

- the request is in writing using the appropriate form (known as Appendix A) signed by a Senior Police Officer, who must cite the relevant exemption/s to the non-disclosure provisions of the Data Protection Act; and
- the police demonstrate that the request is proportionate and necessary for the purposes of a specific crime enquiry. In all other cases the Operations Manager or nominated person will report the request to the Data Controller to seek authorisation to take appropriate action. These procedures will be supported by underpinning guidance which will set out examples of straightforward and justifiable requests and those requiring escalation.

6.3.4. The Operations manager will complete form (see Appendix C & D) to confirm the authenticity of the recordings and arrange for all data on recordings required for disclosure to be copied onto secure encrypted media.

6.3.5. The Operations manager must complete details of the request and any disclosure made in the Incident Report in Selkirk BIDS's Safeguard electronic recording system. For each disclosure request, a copy of the completed police request form, including the reasons given for the request, together with a Selkirk BIDS Disclosure Decision form [Appendix B] recording the decision to withhold or release the information, an encrypted copy of the recording disclosed, where applicable, and reasons for the decision must be lodged with the following responsible officers who maintain a complete confidential record of all such cases on behalf of the Data Protection officer.

6.3.6. Images and recordings requested for police investigations must be supplied directly to the police, not to any third party. Requests by individuals for their own images captured on CCTV will be dealt with in accordance with the section 6.4, below.

6.3.7 The Operations Manager will liaise with the police to ensure that Selkirk BIDS is informed of the outcome of the police investigation and authorise the police to destroy any Selkirk BIDS CCTV images and recordings when they are no longer required.

6.4. Access by Data Subjects

6.4.1. Selkirk BIDS must comply with section 7 of the Data Protection Act, 2018, in informing individuals whether or not images and other information relating to them have been processed by the

SELKIRK BIDS

CCTV PROCEDURES – To support Information Security Policy Framework 30/01/2023

CCTV Surveillance System. Individuals whose images are recorded have a right to make a request to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images. In order to comply with a request, Selkirk BIDS needs to satisfy itself as to the identity of the person making the request for their own personal data. The person making the request also needs to provide enough information to enable Selkirk BIDS staff to locate their images. Therefore, Data Subjects wishing to make a subject access request (request for data about themselves) for CCTV images / recordings / information must apply in writing to the Data Protection Officer at the address given at the end of this Procedure. In the request, the requestor must provide the following information

6.4.1.1. Dates and times of the incident or their visit to Selkirk BIDS with details of the location.

6.4.1.2. Proof of identity (e.g. driving licence/passport containing a photograph); one of these must show your current address

6.4.1.3. Payment of £20.00

6.4.1.4. Whether they require copies or view of the images in question.

6.4.2. A written decision will be sent to the data subject within **14** working days of receipt of the request. If access is agreed, such access will be provided within forty days of receipt of the request or, if later, on the date when Selkirk BIDS receives confirmation of identification from the data subject.

6.4.3. In responding to a subject access request, Selkirk BIDS staff will use red action tools to obscure images of other individuals in cases where releasing the unredacted images would involve an unfair intrusion into the privacy of the third parties concerned. Where Selkirk BIDS is unable to comply with a subject access request without disclosing information relating to another individual who can be identified from that information, it is not obliged to comply with the request unless that individual has consented to the disclosure or it is reasonable, in the circumstances, to comply without the consent of the individual.

SELKIRK BIDS

CCTV PROCEDURES – To support Information Security Policy Framework 30/01/2023

SECTION 7 - COMPLAINTS/BREACHES

7.1. It is also recognised that other members of Selkirk BIDS or third parties may have concerns or complaints in respect to the operation of the CCTV Surveillance System. Any concerns or complaints should, in the first instance, be addressed to the Operations Manager who will follow the Selkirk BIDS Complaints Policy.

7.2. Concerns or queries relating to any aspect of compliance with the Data Protection Act, 1998, (2018) should be directed to the Data Protection Officer.

SECTION 8 - RESPONSIBLE OFFICER

The Operations Manager is responsible for the implementation of these procedures, in consultation with the Data Protection Officer.

SECTION 9 - MONITORING AND REVIEW

The Operations Manager and the Data Protection Officer will monitor compliance with these procedures and the operational effectiveness of the Selkirk BIDS CCTV systems, reporting to the Information Governance and Security Group. These officers will initiate reviews of the procedure out with the annual review cycle where necessary in the light of developments in the current legislation which underpins the procedures. Selkirk BIDS Information Governance and Security Group will review these procedures annually. The review will consider the effectiveness of the procedures and will take account of the views of stakeholders and relevant developments relating to the Data Protection Act, the statutory CCTV Code of Practice and other relevant legislation. Following review, these procedures will be revised and updated as appropriate.

SELKIRK BIDS

CCTV PROCEDURES – To support Information Security Policy Framework 30/01/2023

SECTION 10 - RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

Information Security Policy Framework

SELKIRK BIDS

CCTV PROCEDURES – To support Information Security Policy Framework

CCTV Codes of Practice

SELKIRK BIDS

Code of Practice - Public Space CCTV

Data Protection Policy and Guidance

SELKIRK BIDS

PRIVACY NOTICE

SECTION 11 - FURTHER HELP AND ADVICE

For more information and advice about these procedures contact

Data Protection Officer

SELKIRK BIDS

48 High Street

SELKIRK

TD7 4DD

Email: davcanderson@aol.com

Web: <https://www.exploreselkirk.co.uk>

SELKIRK BIDS

CCTV PROCEDURES – To support Information Security Policy Framework 30/01/2023

SUBJECT ACCESS REQUEST FORM APPENDIX C

Selkirk BIDS – CCTV

DATA PROTECTION ACT 2018 (incorporating GDPR 2018)

How to Apply For Access To Information Held On the SELKIRK BIDS – CCTV System

These notes explain how you can find out what information, if any, is held about you on the CCTV System. Please note that CCTV images are only retained for 28 days.

Your Rights

Subject to certain exemptions, you have a right to be told whether any personal data is held about you. You also have a right to a copy of that information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or if you agree otherwise. NDCC Council will only give that information if it is satisfied as to your identity. If release of the information will disclose information relating to another individual(s), who can be identified from that information, the Council is not obliged to comply with an access request unless –

- The other individual has consented to the disclosure of information, or
- It is reasonable in all the circumstances to comply with the request without the consent of the other individual(s)

SELKIRK BIDS's Rights

Selkirk BIDS may deny access to information where the Regulation allows. The main exemptions in relation to information held on the CCTV System are where the information may be held for: Prevention and detection of crime

- Apprehension and prosecution of offenders
- And giving you the information may be likely to prejudice any of these purposes.

Fee

A fee to deal with this request is £20.00 in most circumstances. Applications can be made using this form

The Application Form: all sections of the form must be completed.

Section 1 Asks you to give information about yourself that will help confirm your identity. Selkirk BIDS has a duty to ensure that information it holds is secure and it must be satisfied that you are who you say you are.

Section 2 Asks you to provide evidence of your identity TWO pieces of ID (e.g. driving licence/passport containing a photograph); one of these must show your current address

Section 3 Asks you to confirm whether you will accept just viewing the information, or if you want a copy of the information.

Section 4 You must sign the declaration

SELKIRK BIDS

CCTV PROCEDURES – To support Information Security Policy Framework 30/01/2023

SUBJECT ACCESS REQUEST FORM APPENDIX D

SELKIRK BIDS CCTV SURVEILLANCE SYSTEM

DATA PROTECTION ACT 2018 (incorporating the GDPR 2018)

SECTION 1 About Yourself

The information requested below is to help NDCC satisfy itself as to your identity and find any data requested

PLEASE USE BLOCK LETTERS

Title (tick box as appropriate) Mr Mrs Miss Ms

Other title (e.g. Dr., Rev., etc.)

Surname/family name

First names

Maiden name/former names

Your Current Home Address

Post Code

A telephone number will be helpful in case you need to be contacted.

Tel. No.

SECTION 2 Proof of Identity

To establish your identity your application must be accompanied by TWO pieces of ID (e.g. driving licence/passport containing a photograph); one of these must show your current address

SECTION 3 Supply of Information

You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form. Do you wish to:

(a) View the information and receive a permanent copy YES/NO

(b) Only view the information YES/NO

SECTION 4 Declaration

DECLARATION (to be signed by the applicant)

The information that I have supplied in this application is correct and I am the person to whom it relates.

Signed by _____

Date ____/____/____

Warning – a person who impersonates or attempts to impersonate another may be guilty of an offence.

This page is intentionally left blank

SELKIRK BIDS

Contents:

- 1. Introduction**
- 2. Good Practice**
- 3. Purpose and Principle**
- 4. Privacy and Data Protection**
- 5. Transparency**
- 6. Control and Operation of Cameras**
- 7. Accountability and Responsibilities**
- 8. Access and Security**

Appendix A: Supportive Information

Appendix B: Owner Information

Section 1 – Introduction

SELKIRK BIDS Public Space Close Circuit TV (CCTV) system are operated by Selkirk BIDS . The scheme covers key local assets and roadways at:

- MUNGO PARK
- TOWER STREET / HIGH STREET JUNCTION
- FLEECE HOTEL (MARKET PLACE)
- WEST PORT
- TOWER STREET / BACK ROW JUNCTION
- POST OFFICE (MARKET PLACE)
- SCOTBET (MARKET PLACE)
- WAR MEMORIAL

Objectives of the System

The 'System' is all activities, processes, procedures that incorporate the management, monitoring, reviewing, and storing of CCTV images.

The objectives of the system as determined for the processing of this data are:

- Prevention, investigation, and detection of crime
- To help with the apprehending and prosecution of offenders
- Increase in public safety and public reassurance
- Add others as appropriate

SELKIRK BIDS believes CCTV is an essential tool it can use to help enhance, provide public reassurance as well as support crime detection and prevention.

The public space CCTV provisions across the community also support Scottish Government aspirations that together deliver the commitment to ensuring our communities continue to be 'safer, better, cleaner and thriving' for all residents and visitors.

- SELKIRK BIDS is the owner of the System
- DAVID ANDERSON is the Data Controller
- SELKIRK BIDS System has been notified to the Information Commissioners Office and is identified by registration number **C1251120**.

Section 2 - Good Practice

Selkirk BIDS has considered relevant principles in relation to the scope and purpose of utilising CCTV, notably that the system will be operated fairly, in accordance with applicable legislation, and only for the purpose for which it is established or agreed in accordance with this Code of Practice. The CCTV System will always be operated with due regard to the privacy of the individual.

Selkirk BIDS recognises that public authorities and those organisations carrying on the functions of a public service nature are required to observe the obligations imposed by the Human Rights Act 1998 and consider that the use of CCTV is a necessary, proportionate, and suitable tool to monitor rivers behaviours, help reduce crime, reduce the fear of crime, and improve public safety.

The Code of Practice and observance of the operational procedures contained in the Operations Manual shall ensure that evidence is secured, retained, and made available as required.

Section 3 – Purpose and Principles

In developing this document, Selkirk BIDS has incorporated the standards and practices from the Information Commissioner’s Office (ICO) Code of Practice covering CCTV and A National Strategy for Public Space CCTV in Scotland (2011) to ensure we work within the law and develop a model of best practice and standards that is consistent to those delivered across the United Kingdom.

This Code of Practice is supplemented by processes and operations contained in the Operations Manual which provides guidelines on all aspects of the day-to-day operation of the System. To ensure the purpose and principles of the CCTV System are realised, the Operations Manual is based upon and expands the contents of the Code.

General Principles of Operation

- The System will be operated in accordance with all the requirements and the principles of the Human Rights Act 1998.
- The System will be operated in accordance with the Data Protection Act 2018 at all times.
- The System will be operated fairly, within the law, and only for the purposes for which it was established and are identified within this Code, or which are subsequently agreed in accordance with this Code of Practice.
- The System will be operated with due regard to the principle that everyone has the right to respect for his or her private and family life and their home.
- The public interest in the operation of the System will be recognised by ensuring the security and integrity of operational procedures.

Throughout this Code of Practice, it is intended, as far as reasonably possible, to balance the objectives of the CCTV System with the need to safeguard the individual’s rights. Every effort has been made throughout the Code to indicate that a formal structure has been put in place, including a complaints procedure, by which it can be identified that the System is not only accountable, but is seen to be accountable.

Cameras and Area Coverage

The areas covered by CCTV to which this Code of Practice refers are key areas within the area of Selkirk.

Cameras offer a view best suited to its purpose at that location.

None of the cameras forming part of the System will be installed in a covert manner.

Monitoring & Recording Facilities

Selkirk BIDS CCTV system will only be viewed by appointed/trained Selkirk BIDS appointees. Selkirk BIDS appointees will be:

Chair of Selkirk BIDS – David Anderson
Director of Selkirk BIDS – Stuart Davidson
Director of Selkirk BIDS – Vivienne Ross

Viewing will be made by the nominated individuals for reasons detailed in the **Objectives of the system** in Section 1 of this document. Cameras record over a period of 24 hours per day/seven days per week.

This Code is intended to provide a framework for the delivery of good practice for Selkirk BIDS and appointees who are involved in managing and operating Public Space CCTV.

CCTV operators can record images, produce copies of recorded images, replay, or copy any pre-recorded data at their discretion (with authorisation) and in accordance with the Code of Practice. All viewing and recording equipment shall only be operated by trained and authorised users.

Information that relates to a person is deemed as personal data as such the management of this data is subject to the protection and provisions of the Data Protection Act 2018 (DPA) updated 2020 and the exemptions therein.

Management of CCTV data complies fully with the legal requirements of the DPA.

Human Resources

Unauthorised persons will not have access without an authorised member of Selkirk BIDS being present. Monitoring shall be undertaken by trained operators in accordance with the industry and accreditation standards.

All operators receive training relevant to their role in the requirements of the relevant legislation and the Codes of Practice and Operations Manual. Further training will be provided as necessary.

Processing and Handling of Recorded Material

Every request for the release of personal data generated by this CCTV System will be channelled through the appointed Data Controller. In complying with the national standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individual's rights to privacy and to give effect to the following principles:

- Recorded material shall be processed lawfully and fairly and used only for the purposes defined in this Code of Practice.
- All recorded material will be processed and handled strictly in accordance with this Code of Practice and the Operations Manual.
- Recorded data will be used only for the purposes defined in the Code of Practice and relevant legislative requirements.
- Recorded data will be kept for a maximum of 28 days before being erased unless required for a specific enquiry or for archiving the monitoring of river levels (in this instance 90 days before erasing)
- Access to recorded data will only take place as defined in the Code of Practice and relevant legislation.
- In particular, recorded personal data will not be sold or used for commercial purposes or the provision of entertainment.
- The type of data recording for storage used is digital hard drives.

Several legally enforceable principles apply to this section, notably:

- Recorded data may be used in court as evidence. It must be of good quality and be accurate in content. Recorded data must be treated according to defined procedures to provide continuity of evidence and to avoid contamination of this evidence.
- Appropriate security measures shall be taken against the unauthorised access to, alteration of, disclosure of and against accidental loss or destruction of, recorded data.
- Recorded data should be held only for the purposes provided by this Code of Practice and relevant legislation.
- Information recorded should be accurate, adequate, and relevant and not exceed that necessary to fulfil the purposes and key objectives of this Code of Practice.
- Recorded data shall be kept no longer than is necessary for the purposes and key objectives of the scheme. It must then be securely destroyed.
- Members of the public must be confident that information recorded about their ordinary activities in the area covered by the cameras is treated with due regard to their individual privacy.

Data Management

- All the CCTV footage is stored in a secure location.
- All data is automatically erased after the required retention period, with the exception of river level monitoring data as detailed.
- Relevant security protocols and levels are applied to all CCTV footage.
- Any images transferred to Police Scotland or other relevant agency is done so in a secure and proportionate manner.

Operators Instructions

Technical instructions on the use of equipment housed within the monitoring stations are contained in a separate manual provided by the equipment suppliers.

Section 4 – Privacy and Data Protection

Information Commissioner’s Office

David Anderson is registered with the Information Commissioner’s Office (ICO) as the data controller for the information gathered and managed through the Public Space CCTV System. ICO Registration Number **C1251120**.

Data Protection Legislation

Selkirk BIDS delivers the management of data in compliance with the DPA. Key principles of the DPA concerning the processing of data include the following:

- All personal data will be obtained and processed fairly and lawfully.
- Personal data will be held only for the purposes specified.
- Personal data will be used only for the purposes, and disclosed only to the people, shown within these codes of practice.
- Only personal data will be held which is adequate, relevant and not excessive in relation to the purpose for which the data is held.
- Steps will be taken to ensure that personal data is accurate and where necessary, kept up to date.
- Personal data will be held for no longer than is necessary.
- Individuals will be allowed access to information held about them and, where appropriate, permitted to correct or erase it.
- Procedures will be implemented to put in place security measures to prevent unauthorised or accidental access to, alteration, disclosure or loss and destruction of information.

Personal Data

Selkirk BIDS is fully compliant with the lawful reasons for processing Personal Data, as detailed under Schedule 2 of the DPA:

Procedures will be implemented to deliver security measures to prevent unauthorised or accidental access to, alteration, disclosure or loss and destruction of information.

- The Data Subject has consented (appropriate signage erected to denote CCTV coverage).
- Processing is necessary for the purposes of legitimate interests pursued by the appointed Data Controller and third-party discloser’s and does not prejudice the rights and freedoms and legitimate interests of others and with the lawful reasons for processing Sensitive Personal Data, under Schedule 3 of the Act, wherein the process:
 - Is in the substantive public interest.
 - Is necessary for the purposes of the prevention and detection of any unlawful act.
 - Must necessarily be carried out without the explicit consent of the data subjects so as not to prejudice those purposes.

CCTV Data

Selkirk BIDS will use the CCTV and the data collected therein, for the following approved purposes:

- Prevention, investigation, and detection of crime.
- To help with the increased apprehending and prosecution of offenders.
- Risk management and environmental concerns.
- Increase in public safety and public reassurance.
- Others added as appropriate

The storage, security and processing of the data will be strictly in accordance with the requirements of the Data Protection Act 2018 and additional locally agreed procedures.

Note: ‘Processing’ means obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the information or data, including:

1. Organisation, adaptation or alteration of the information or data.

2. Retrieval, consultation or use of the information or data.
3. Disclosure of the information or data by transmission, dissemination or otherwise making available, or
4. Alignment, combination, blocking, erasure, or destruction of the information.

Disclosure

Disclosure of images from CCTV will be controlled and consistent with the purpose for which the System was established. Selkirk BIDS will ensure that any external agency that receives disclosed information are fully aware of and accept their responsibilities as outlined in the DPA

Responsibilities

Selkirk BIDS is the data controller for the data collected through the Public Space CCTV System. All nominated staff will be Disclosure Checked in accordance with current Legislation and training will be given on GDPR.

Making a request for CCTV footage

Individuals whose images are recorded have a right to request access to view relevant footage and, where appropriate provided with a copy of the images in a still or virtual format. Should a data subject or his/her authorised representative believe that (name) may hold CCTV footage of them, they are entitled to request access to this data under Schedule 2 of the DPA. To access to CCTV footage, an individual must:

- make the request in writing providing a reason for accessing the data
- supply appropriate information to help locate the required footage.

Processing a request

In the first instance, an authorised person will check whether the area in question is covered by the Public Space CCTV. If the area is not covered, the requestor will be informed as soon as possible, and the case will be closed.

If the area is covered by Public Space CCTV, the requestor will be provided with a Subject Access Request form. The Subject Access Request seeks evidence of the enquirers identity. An application must be accompanied by TWO pieces of ID (e.g. driving licence/passport containing a photograph); one of these must show your current address as well as provide the details regarding the footage they wish to access (e.g. time, date, location, reason).

At this time the requestor will also be advised that footage is only held for a maximum period of 28 days before it is considered for disposal, unless there is a specific reason to retain it for an extended period. The individual can decide whether to proceed or not, depending on the time elapsed since the incident of which footage is sought.

A fully completed Subject Access Request form, along with documentation is required within 14 days of issue or the case will be closed.

The Data Controller will consider extensions on a case- by-case basis.

A search for footage will commence on receipt of all necessary documents and a response will be provided to the requestor within 40 calendar days. Possible outcomes are:

- Footage found/not found
- Out of time (footage deleted after a maximum of 28 days)
- Footage already passed to Police/Procurator Fiscal
- Camera non-functional

Providing access to footage

If footage is found the Data Controller will decide if any of the footage contains images of third parties and whether access to or release of the footage would violate the data protection rights of the third party or parties.

Where it has been deemed appropriate to allow access to the footage, the data subject, or their representative, will be invited to view the footage at a location decided by (name). Where it has not been deemed appropriate to allow footage to be viewed, the data subject may be provided with a narrative of the footage content or a still photographic form, where appropriate.

If access is denied completely, the Data Controller will inform the data subject of the decision and the reason, in writing.

They will also be informed of:

- Any process available to him/her to appeal this decision.
- How to make a complaint to the Information Commissioner's Officer, in addition to processing an appeal.

Contact details:

As appropriate

Freedom of information (FOI)

As a public body, Selkirk BIDS is subject to the Freedom of Information (Scotland) Act 2002 (FOISA).

FOI requests to Secretary in relation to Public Space CCTV provision can include information on where cameras are sited, functionality, and whether they were operational over particular periods.

All FOI requests have to be in a permanent format either by letter / email or via the (name)

Contact details for the FOI officer are:

Freedom of Information Officer

Email:

Requests for information are processed within 20 working days from the acknowledgment of an appropriate request.

Access to CCTV images captured may be subject to an exemption under Section 38 of the Freedom of Information (Scotland) Act 2018.

Section 5 – Transparency

Selkirk BIDS will ensure the recording and retention of images (sensitive personal data) of people in public places shall be undertaken fairly and lawfully in accordance with DPA.

Selkirk BIDS will ensure that the public are aware that their image is being recorded through static cameras and that the identity of the owner of the System (name) is clearly visible.

The visibility of ownership and purpose of the cameras will be provided by ensuring:

Prominent signs are placed where the CCTV cameras are in operation with relevant details on how Selkirk BIDS can be contacted. Signage will be:

- Clearly visible, readable and appropriate in size also containing contact information.
- Indicates that CCTV cameras are in operation and are displayed at appropriate locations covered by the scheme allowing people entering the area to make an appropriate approximation of the CCTV camera coverage area.
- If vandalised or removed the signs will be replaced as soon as reasonably possible.

All persons operating the cameras must adhere to this Code of Practice and requirements of the DPA.

Only approved Selkirk BIDS appointees or persons who have SIA CCTV accreditation will operate the cameras (there will be exception for Police Scotland officers trained in the use of CCTV)

Every use of the camera will accord with the purpose and key objectives of the System and shall be compliant with this code. Cameras will not be used to investigate private residential property, 'privacy zones' will be programmed into the System.

Selkirk BIDS will adhere to the following core principles:

Guiding Principles

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must consider its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held, and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

Section 6 – Control and Operation of Cameras

Primary Control

Only those trained and authorised by (name) with responsibility for using the CCTV equipment will have access to the operating controls, those operators have primacy of control at all times.

Maintenance of the System

To ensure compliance with the Information Commissioners Office Code of Practice and that images recorded continue to be of appropriate evidential quality, the CCTV System shall be maintained in accordance with the manufacturer's requirements.

Maintenance schedule will make provision for regular/periodic service checks on the equipment which will include cleaning of any all-weather domes or housings, checks on the functioning of the equipment, and any minor adjustments that need to be made to the equipment settings to maintain picture quality.

The maintenance will also include regular periodic overhaul of all the equipment and replacement of equipment which is reaching the end of its serviceable life.

It is the responsibility of the operator to ensure appropriate records are maintained in respect of the functioning of the cameras and the response of the maintenance organisation.

Authorised Access

Only authorised personnel will operate the equipment or equipment associated with the System.

Public Access

Public access to the System will be prohibited except for lawful, proper, and sufficient reasons. Any such visits will be conducted and recorded in accordance with the procedure manual.

Security

Authorised personnel will be always present when images are viewed. The monitoring facility is to be secured at all times

In accordance with the legal responsibilities, of the DPA and Regulation of Investigatory Powers (Scotland) Act 2000:

- The operation and management of the public space CCTV provision, along with the process for collection, management and securing of personal data collected through this provision is registered with the Information Commissioners Office annually.
- The CCTV System is operated in compliance with the current Code of Practice issued by the Information Commissioner in respect of the operation of CCTV in public places.
- Appropriate signage will be erected to notify the public of the presence of CCTV cameras and recording equipment. These signs will carry the necessary information prescribed in the Information Commissioner's Code of Practice.
- (name) will undertake an annual audit of CCTV practises to ensure compliance with the DPA and Information Commissioners Office (ICO) Code of Practice.

Effective management of the CCTV System requires that:

- Access to all the data held, and the CCTV equipment, should comply with specific guidelines as highlighted in this code.
- The Operational Manual and documentation required to run this scheme must be developed from, and specifically linked to, this Code of Practice.
- All incidents witnessed on the CCTV System or on review of a recording will be logged.
- Data shall be stored for a maximum of 28 days before being digitally erased unless required for a specific enquiry (Flood management data will be stored for 90 days)
- All CCTV equipment will be kept in good working order and serviced according to manufacturer recommendations.
- When a fault develops on the CCTV System, it shall be recorded on the fault management system and the appropriate action taken to ensure a speedy repair.
- All CCTV equipment shall be secured to prevent interference from unauthorised personnel. This means that recording equipment shall be kept in a secure environment, which is a controlled and secure location.
- CCTV data shall be afforded a high level of security. Access to recordings shall be limited to (name) appointees authorised by the Data Controller.
- All CCTV data will be stored in a secure environment to prevent unauthorised or unlawful processing of personal data and against accidental loss, damage, or destruction of personal data.
- Any data held for evidential purposes will be kept away from other personal data in a secure location.
- No unauthorised copies will be made of any personal data except with the permission of the (name) Data Controller. They shall record the reason and ensure that all copies are numbered and only disclosed to authorised parties. The Data Controller shall also ensure personal data is not kept for longer than necessary and it destroyed as if it were an original recording.
- No guarantee is given or implied that any incident will be observed and recorded by the System. However, all CCTV Operators and management will endeavour to provide a level of coverage based on up-to-date information concerning incidents and activities commensurate within the purposes of the CCTV System.
- Cameras will not be used to view into private residential property.

- Where the equipment permits it 'privacy Zones' and blackouts will be programmed into the System as required, in order to ensure that the interior of any private residential property within the range of the System is not surveyed by the cameras. All operators are fully trained in privacy issues and requirements.

It should also be acknowledged that constraints are placed upon every CCTV system by the limits of current technology.

Section 7 - Accountability and Responsibilities

Selkirk BIDS Authorised Appointees will have unrestricted access to the control stations and System.

Selkirk BIDS Authorised Appointees will ensure that any issues, concerns of complaint are dealt with in an appropriate and timely manner.

Selkirk BIDS will have day to day responsibility for the management and maintenance of the System.

The System will be subject to regular reviews and audits.

Human resources

Selkirk BIDS Authorised Appointees are fully trained in the use of the CCTV System and must adhere to the regulations and governance in place. A regular review of regulatory guidance will be undertaken.

All appointees will be provided with copies of this code and relevant documents to ensure adherence with the code and associated procedures. Each individual (having responsibility under the terms of this code) who is involved with the system to which it refers will be subject to the organisations policies and procedures. Any breach of this code or any aspect of confidentiality will be dealt with in accordance with the relevant policy.

8 - Access and Security

Authorised Access

Only trained and authorised personnel will operate any of the equipment located within the CCTV monitoring stations, (or equipment associated with the CCTV System).

Public access

Public access to the monitoring and recording facility is restricted except for lawful, proper, and sufficient reasons and only then with the personal authority of the (name) . Any such visits will be conducted and recorded in accordance with the Operations Manual.

Security

Authorised personnel will be always present when the equipment is in use. If the monitoring facility is to be left unattended for any reason it will be secured.

Supportive Information

The Information Commissioners Office (ICO) is responsible for ensuring Data Protection Rights are observed across the United Kingdom. The contact details for the ICO are:

Information Commissioner's Office (Scotland) 45 Melville Street, Edinburgh, EH3 7HL

Tel: 0131 244 9001

Helpline: 0303 123 1113

Email: scotland@ico.gsi.gov.uk Web site:

<https://www.ico.gov.uk/> Use of CCTV Provisions and Data Protection

Information is available to the general public on their rights at <https://ico.org.uk/for-the-public/>

Appendix B

Owner Information

Data Controller: David Anderson

Authorised System Owners – SELKIRK BIDS

System Maintenance: POSITEC (UK) LTD

Contact details: 07778 514150 peter.stanhope@positec-ltd.com

This page is intentionally left blank

SELKIRK BIDS – DESTRUCTION POLICY 30.01.23

DESTRUCTION POLICY

In specific circumstances, data subjects' have the right to request that their personal data is erased. However, Selkirk BIDS recognise that this is not an absolute 'right to be forgotten'. Data subjects only have a right to have personal data erased and to prevent processing if one of the below conditions applies:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data must be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

Where one of the above conditions applies and Selkirk BIDS received a request to erase data, we first ensure that no other legal obligation or legitimate interest applies. If we are confident that the data subject has the right to have their data erased, this is carried out under instruction by the Data Protection Officer in conjunction the IT team to ensure that all data relating to that individual has been erased.

These measures enable us to comply with a data subject's right to erasure, whereby an individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing. Whilst our standard procedures already remove data that is no longer necessary, we still follow a dedicated process for erasure requests to ensure that all rights are complied with and that no data has been retained for longer than is needed.

SELKIRK BIDS – DESTRUCTION POLICY 30.01.23

Where Selkirk BIDS receive a request to erase and/or remove personal information from a data subject, the below process is followed:

1. The request is allocated to the Data Protection Officer and recorded on the Data Erasure Request Register
2. The DPO locates all personal information relating to the data subject and reviews it to see if it is still being processed and is still necessary for the legal basis and purpose it was originally intended
3. The request is reviewed to ensure it complies with one or more of the grounds for erasure: -
 - the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
 - the data subject has withdrawn consent on which the processing is based and where there is no other legal ground for the processing
 - the data subject objects to the processing and there are no overriding legitimate grounds for the processing
 - the personal data has been unlawfully processed
 - the personal data must be erased for compliance with a legal obligation
 - the personal data has been collected in relation to the offer of information society services to a child
4. If the erasure request complies with one of the above grounds, it is erased within 28 days of the request being received
5. The DPO writes to the data subject and notifies them in writing that the right to erasure has been granted and provides details of the information erased and the date of erasure
6. Where Selkirk BIDS has made any of the personal data public and erasure is granted, we will take every reasonable step and measure to remove public references, links and copies of data and to contact related controllers and/or processors and inform them of the data subjects request to erase such personal data

SELKIRK BIDS – DESTRUCTION POLICY 30.01.23

If for any reason, we are unable to act in response to a request for erasure, we always provide a written explanation to the individual and inform them of their right to complain to the ICO to a judicial remedy. Such refusals to erase data include:

- Exercising the right of freedom of expression and information
- Compliance with a legal obligation for the performance of a task carried out in the public interest
- For reasons of public interest in the area of public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing
- For the establishment, exercise or defence of legal claims

Special Category Data

In accordance with GDPR requirements and Schedule 1 Part 4 of The Data Protection Act 2018, organisations are required to have and maintain appropriate policy documents and safeguarding measures for the retention and erasure of special categories of personal data and criminal convictions etc.

Our methods and measures for destroying and erasing data are noted in this policy and apply to all forms of records and personal data, as noted in our Data Retention policy.

Compliance and Monitoring

Selkirk BIDS is committed to ensuring the continued compliance with this policy and any associated legislation and undertake regular audits and monitoring of our records, their management, archiving and retention. Information asset owners are tasked with ensuring the continued compliance and review of records and data within their remit.

Responsibilities

Selkirk BIDS Data Protection Officer has overall responsibility for the management of records and data generated by the council's activities namely, to ensure that the records created, received and controlled within the purview of their organisation, and the systems (electronic or otherwise) and procedures they adopt, are managed in a way which meets the aims of this policy.

Where a DPO has been designated, they must be involved in any data retention processes and records or all archiving and destructions must be retained. Individual volunteers/employees must ensure that the records for which they are responsible are complete and accurate records of their activities, and that they are maintained and disposed of in accordance with Selkirk BIDS protocols.

Prior to the destruction of any documents, confirmation should be sought from the DPO.

SELKIRK BIDS – DESTRUCTION POLICY 30.01.23

Data destruction

Selkirk BIDS has processes in place to ensure any personal and confidential is destroyed securely (including at the end of data retention periods).

- On-site paper shredder for secure shredding
- Confidential waste collection from a certified third party.
- Once deleted from the online database recycle bin, individual data records cannot be retrieved by users.
- Electronic files deleted from company servers are only recoverable by third party IT service provider.
- CCTV footage is deleted/overwritten after 28 days (with the exception of flood information which will be retained for 90 days)

FURTHER HELP AND ADVICE

For more information and advice about this policy contact

Data Protection Officer

Selkirk BIDS

48 High Street

Selkirk

TD7 4DD

Email: DAVCANDERSON@AOL.COM

Web: <https://www.exploreselkirk.co.uk>

ICO Scotland contact details

The Information Commissioner's Office – Scotland

Queen Elizabeth House

Sibbald Walk

Edinburgh

EH8 8FT

Telephone: 0303 123 1115

Email: Scotland@ico.org.uk

Contents:

- 1. Introduction**
- 2. Good Practice**
- 3. Purpose and Principle**
- 4. Privacy and Data Protection**
- 5. Transparency**
- 6. Control and Operation of Cameras**
- 7. Accountability and Responsibilities**
- 8. Access and Security**

Appendix A: Supportive Information

Appendix B: Owner Information

SECTION 1 – INTRODUCTION

Newcastleton Public Space Close Circuit TV (CCTV) system are operated by Newcastleton & District Community Council (NDCC). The scheme covers key local assets and roadways at:

- Western Roadside Entrance to village
- Dalkeith House (covers Langholm Road entrance to village)
- The Grapes Hotel
- The Spar retail shop and Post Office
- Newcastleton Primary School
- Whithaugh Pool on riverside
- Eastern Roadside Entrance to village

Objectives of the System

The 'System' is all activities, processes, procedures that incorporate the management, monitoring, reviewing, and storing of CCTV images.

The objectives of the system as determined by NDCC forming the lawful basis for the processing of this data are:

- For the purposes of monitoring river levels for flood prevention
- Water safety and management
- Prevention, investigation, and detection of crime
- To help with the apprehending and prosecution of offenders
- Increase in public safety and public reassurance

NDCC believes CCTV is an essential tool it can use to help enhance local flood prevention, provide public reassurance as well as support crime detection and prevention. Our remote rural location can be a magnet for rural crime, our roadways and forest tracks are often used as a gateway to cross from England into Scotland and vice versa.

The public space CCTV provisions across the community also support Scottish Government aspirations that together deliver the commitment to ensuring our communities continue to be 'safer, better, cleaner and thriving' for all residents and visitors.

- Newcastleton & District Community Council is the owner of the System
- Newcastleton & District Community Council is the Data Controller
- The Newcastleton & District Community Council System has been notified to the Information Commissioners Office and is identified by registration number Z2914994

SECTION 2 - GOOD PRACTICE

NDCC has considered relevant principles in relation to the scope and purpose of utilising CCTV, notably that the system will be operated fairly, in accordance with applicable legislation, and only for the purpose for which it is established or agreed in accordance with this Code of Practice. The CCTV System will always be operated with due regard to the privacy of the individual.

NDCC recognises that public authorities and those organisations carrying on the functions of a public service nature are required to observe the obligations imposed by the Human Rights Act 1998 and consider that the use of CCTV is a necessary, proportionate, and suitable tool to monitor rivers levels, help reduce crime, reduce the fear of crime, and improve public safety.

The Code of Practice and observance of the operational procedures contained in the Operations Manual shall ensure that evidence is secured, retained, and made available as required.

SECTION 3 – PURPOSE AND PRINCIPLES

In developing this document, NDCC has incorporated the standards and practices from the Information Commissioner’s Office (ICO) Code of Practice covering CCTV and A National Strategy for Public Space CCTV in Scotland (2011) to ensure we work within the law and develop a model of best practice and standards that is consistent to those delivered across the United Kingdom.

This Code of Practice is supplemented by processes and operations contained in the Operations Manual which provides guidelines on all aspects of the day-to-day operation of the System. To ensure the purpose and principles of the CCTV System are realised, the Operations Manual is based upon and expands the contents of the Code.

General Principles of Operation

- The System will be operated in accordance with all the requirements and the principles of the Human Rights Act 1998.
- The System will be operated in accordance with the Data Protection Act 2018 at all times.
- The System will be operated fairly, within the law, and only for the purposes for which it was established and are identified within this Code, or which are subsequently agreed in accordance with this Code of Practice.
- The System will be operated with due regard to the principle that everyone has the right to respect for his or her private and family life and their home.
- The public interest in the operation of the System will be recognised by ensuring the security and integrity of operational procedures.

Throughout this Code of Practice, it is intended, as far as reasonably possible, to balance the objectives of the CCTV System with the need to safeguard the individual’s rights. Every effort has been made throughout the Code to indicate that a formal structure has been put in place, including a complaints procedure, by which it can be identified that the System is not only accountable, but is seen to be accountable.

Cameras and Area Coverage

The areas covered by CCTV to which this Code of Practice refers are key areas within the area of NDCC.

Cameras offer a view best suited to its purpose at that location.

None of the cameras forming part of the System will be installed in a covert manner.

Monitoring & Recording Facilities

Newcastleton CCTV system can only be viewed by appointed and trained NDCC appointees.

NDCC appointees will be

Chair of NDCC – Presently Greg Cuthbert

Chair of Newcastleton Resilience Group – Presently Pauline Elliot

Data Controller of NDCC – Presently Barbara Elborn

Viewing will be made by the nominated individuals for reasons detailed in the “Objectives of the system” in Section 1 of this document and in the case of a potential flooding incident Scottish Borders Emergency Planning Services may be included in the viewing. Cameras record over a period of 24 hours per day/seven days per week.

This Code is intended to provide a framework for the delivery of good practice for NDCC and appointees who are involved in managing and operating Public Space CCTV.

CCTV operators can record images, produce copies of recorded images, replay, or copy any pre-recorded data at their discretion (with authorisation) and in accordance with the Code of Practice. All viewing and recording equipment shall only be operated by trained and authorised users.

Information that relates to a living person is deemed as personal data as such the management of this data is subject to the protection and provisions of the Data Protection Act 2018 (DPA) updated 2020 and the exemptions therein.

Management of CCTV data complies fully with the legal requirements of the DPA.

Human Resources

Unauthorised persons will not have access without an authorised member of NDCC being present.

Monitoring shall be undertaken by trained operators in accordance with the industry and accreditation standards.

All operators shall receive training relevant to their role in the requirements of the relevant legislation and the Codes of Practice and Operations Manual. Further training will be provided as necessary.

Processing and Handling of Recorded Material

Every request for the release of personal data generated by this CCTV System will be channelled through the appointed Data Controller.

In complying with the national standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individual's rights to privacy and to give effect to the following principles:

- Recorded material shall be processed lawfully and fairly and used only for the purposes defined in this Code of Practice.
- All recorded material will be processed and handled strictly in accordance with this Code of Practice and the Operations Manual.
- Recorded data will be used only for the purposes defined in the Code of Practice and relevant legislative requirements.
- Recorded data will be kept for a maximum of 28 days before being erased unless required for a specific enquiry or for archiving the monitoring of river levels (in this instance 90 days before erasing)
- Access to recorded data will only take place as defined in the Code of Practice and relevant legislation.
- In particular, recorded personal data will not be sold or used for commercial purposes or the provision of entertainment.
- The type of data recording for storage used is digital hard drives.

Several legally enforceable principles apply to this section, notably:

- Recorded data may be used in court as evidence. It must be of good quality and be accurate in content. Recorded data must be treated according to defined procedures to provide continuity of evidence and to avoid contamination of this evidence.
- Appropriate security measures shall be taken against the unauthorised access to, alteration of, disclosure of and against accidental loss or destruction of, recorded data.
- Recorded data should be held only for the purposes provided by this Code of Practice and

relevant legislation.

- Information recorded should be accurate, adequate, and relevant and not exceed that necessary to fulfil the purposes and key objectives of this Code of Practice.
- Recorded data shall be kept no longer than is necessary for the purposes and key objectives of the scheme. It must then be securely destroyed.
- Members of the public must be confident that information recorded about their ordinary activities in the area covered by the cameras is treated with due regard to their individual privacy.

Data Management

- All the CCTV footage is stored in a secure location.
- All data is automatically erased after the required retention period, with the exception of river level monitoring data as detailed.
- Relevant security protocols and levels are applied to all CCTV footage.
- Any images transferred to Police Scotland or other relevant agency is done so in a secure and proportionate manner.

Operators Instructions

Technical instructions on the use of equipment housed within the monitoring stations are contained in a separate manual provided by the equipment suppliers.

SECTION 4 – PRIVACY AND DATA PROTECTION

Information Commissioner’s Office

Newcastleton & District Community Council is registered with the Information Commissioner’s Office (ICO) as the data controller for the information gathered and managed through the Public Space CCTV System. ICO Registration Number Z2914994

Data Protection Legislation

NDCC delivers the management of data in compliance with the Data Protection Act 2018 (DPA). Key principles of the DPA concerning the processing of data include the following:

- All personal data will be obtained and processed fairly and lawfully.
- Personal data will be held only for the purposes specified.
- Personal data will be used only for the purposes, and disclosed only to the people, shown within these codes of practice.
- Only personal data will be held which is adequate, relevant and not excessive in relation to the purpose for which the data is held.
- Steps will be taken to ensure that personal data is accurate and where necessary, kept up to date.
- Personal data will be held for no longer than is necessary.
- Individuals will be allowed access to information held about them and, where appropriate, permitted to correct or erase it.
- Procedures will be implemented to put in place security measures to prevent unauthorised or accidental access to, alteration, disclosure or loss and destruction of information.

Personal Data

NDCC is fully compliant with the lawful reasons for processing Personal Data, as detailed under Schedule 2 of the Data Protection Act 2018:

Procedures will be implemented to deliver security measures to prevent unauthorised or accidental access to, alteration, disclosure or loss and destruction of information.

- The Data Subject has consented (appropriate signage erected to denote CCTV coverage).
- Processing is necessary for the purposes of legitimate interests pursued by the appointed Data Controller and third-party discloser’s and does not prejudice the rights and freedoms and legitimate interests of others and with the lawful reasons for processing Sensitive Personal Data, under Schedule 3 of the Act, wherein the process:
 - Is in the substantive public interest.
 - Is necessary for the purposes of the prevention and detection of any unlawful act.
 - Must necessarily be carried out without the explicit consent of the data subjects so as not to prejudice those purposes.

CCTV Data

NDCC will use the CCTV and the data collected therein, for the following approved purposes:

- For the purposes of monitoring river levels for flood prevention.
- Water safety and management.
- Prevention, investigation, and detection of crime.
- To help with the increased apprehending and prosecution of offenders.
- Risk management and environmental concerns.

- Increase in public safety and public reassurance.

The storage, security and processing of the data will be strictly in accordance with the requirements of the Data Protection Act 2018 and additional locally agreed procedures.

Note: 'Processing' means obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the information or data, including.

1. Organisation, adaptation or alteration of the information or data.
2. Retrieval, consultation or use of the information or data.
3. Disclosure of the information or data by transmission, dissemination or otherwise making available, or
4. Alignment, combination, blocking, erasure, or destruction of the information.

Disclosure

Disclosure of images from CCTV will be controlled and consistent with the purpose for which the System was established.

NDCC will ensure that any external agency that receives disclosed information are fully aware of and accept their responsibilities as outlined in the Data Protection Act 2018.

Responsibilities

NDCC is the data controller for the data collected through the Public Space CCTV System. All nominated staff will be Disclosure Checked in accordance with current Legislation and training will be given on GDPR.

Making a request for CCTV footage

Individuals whose images are recorded have a right to request access to view relevant footage and, where appropriate, to be provided with a copy of the images in a still or virtual format.

Should a data subject or his/her authorised representative believe that NDCC may hold CCTV footage of them, they are entitled to request access to this data under Schedule 2 of the DPA. To access to CCTV footage, an individual must:

- make the request in writing providing a reason for accessing the data
- supply appropriate information to help locate the required footage.

Processing a request

In the first instance, an authorised person will check whether the area in question is covered by the Public Space CCTV. If the area is not covered, the requestor will be informed as soon as possible, and the case will be closed.

If the area is covered by Public Space CCTV, the requestor will be provided with a Subject Access Request form. The Subject Access Request seeks evidence of your identity. An application must be accompanied by TWO pieces of ID (e.g. driving licence/passport containing a photograph); one of these must show your current address as well as provide the details regarding the footage they wish to access (e.g. time, date, location, reason).

At this stage, the requestor will also be advised that CCTV footage is held for a maximum period of 28 days before it is considered for disposal, unless there is a specific reason to retain it for an extended period. The individual can decide whether to proceed or not, depending on the time elapsed since the

incident of which footage is sought.

A fully completed Subject Access Request form, along with documentation is required within 14 days of issue or the case will be closed.

The Data Controller will consider extensions on a case- by-case basis.

A search for footage will commence on receipt of all necessary documents and a response will be provided to the requestor within 40 calendar days. Possible outcomes are:

- Footage found
- Footage not found
- Out of time (footage deleted after a maximum of 28 days)
- Footage already passed to Police/Procurator Fiscal
- Camera non-functional

Providing access to footage

If footage is found the Data Controller will decide if any of the footage contains images of third parties and whether access to or release of the footage would violate the data protection rights of the third party or parties.

Where it has been deemed appropriate to allow access to the footage, the data subject, or their representative, will be invited to view the footage at a location decided by NDCC. Where it has not been deemed appropriate to allow footage to be viewed, the data subject may be provided with a narrative of the footage content or a still photographic form, where appropriate.

If access is denied completely, the Data Controller will inform the data subject of the decision and the reason, in writing. They will also be informed of:

- Any process available to him/her to appeal this decision.
- How to make a complaint to the Information Commissioner's Officer, in addition to processing an appeal.

Contact details:

secretary@newcastletoncommunitytrust.co.uk

Freedom of information (FOI)

As a public body, Newcastleton & District Community Council is subject to the Freedom of Information (Scotland) Act 2002 (FOISA).

FOI requests to Secretary in relation to Public Space CCTV provision can include information on where cameras are sited, functionality, and whether they were operational over particular periods.

All FOI requests have to be in a permanent format either by letter / email or via the Secretary of Newcastleton & District Community Council.

The contact details for the FOI officer are:

Freedom of Information Officer

Email: secretary@newcastletoncommunitytrust.co.uk

Website: <https://www.visitnewcastleton.com/>



NEWCASTLETON DISTRICT COMMUNITY COUNCIL
Newcastleton Public Space CCTV - CODE OF PRACTICE – 02.03.22

Requests for information are processed within 20 working days from the acknowledgment of an appropriate request.

Access to CCTV images captured may be subject to an exemption under Section 38 of the Freedom of Information (Scotland) Act 2018.

SECTION 5 – TRANSPARENCY

Newcastleton & District Community Council will ensure the recording and retention of images (sensitive personal data) of people in public places shall be undertaken fairly and lawfully in accordance with Data Protection Act 2018 (DPA).

NDCC will ensure that the public are aware that their image is being recorded through static cameras and that the identity of the owner of the System (NDCC) is clearly visible.

The visibility of ownership and purpose of the cameras will be provided by ensuring:

Prominent signs are placed where the CCTV cameras are in operation with relevant details on how NDCC can be contacted. Signage will be:

- Clearly visible and readable and appropriate in size.
- Contains contact information.
- Indicates that CCTV cameras are in operation and is displayed at appropriate locations covered by the scheme to allow people entering the area to make an appropriate approximation of the CCTV camera coverage area.
- If vandalised or removed the signs will be replaced as soon as reasonably possible.

All persons operating the cameras must adhere to this Code of Practice and requirements of the Data Protection Act 2018.

Only approved Newcastleton & District Community Council appointees or persons who have SIA CCTV accreditation will operate the cameras (there will be exception for Police Scotland officers trained in the use of CCTV)

Every use of the camera will accord with the purpose and key objectives of the System and shall be compliant with this code.

Cameras will not be used to investigate private residential property.

Where the equipment permits and if required 'privacy zones' will be programmed into the System.

Newcastleton & District Community Council will adhere to the following core principles:

Guiding Principles

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must consider its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the

stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

SECTION 6 – CONTROL AND OPERATION OF CAMERAS

Primary Control

Only those trained and authorised by Newcastleton & District Community Council with responsibility for using the CCTV equipment will have access to the operating controls, those operators have primacy of control at all times.

Maintenance of the System

To ensure compliance with the Information Commissioners Office Code of Practice and that images recorded continue to be of appropriate evidential quality, the CCTV System shall be maintained in accordance with the manufacturer's requirements.

Maintenance schedule will make provision for regular/ periodic service checks on the equipment which will include cleaning of any all-weather domes or housings, checks on the functioning of the equipment, and any minor adjustments that need to be made to the equipment settings to maintain picture quality.

The maintenance will also include regular periodic overhaul of all the equipment and replacement of equipment which is reaching the end of its serviceable life.

It is the responsibility of the operator to ensure appropriate records are maintained in respect of the functioning of the cameras and the response of the maintenance organisation.

Authorised Access

Only authorised personnel will operate the equipment located within the control room or equipment associated with the System.

Public Access

Public access to the System will be prohibited except for lawful, proper, and sufficient reasons. Any such visits will be conducted and recorded in accordance with the procedure manual.

Security

Authorised personnel will be always present when images are viewed. The monitoring facility is to be secured at all times. In accordance with the legal responsibilities, of the Data Protection Act 2018 and Regulation of Investigatory Powers (Scotland) Act 2000:

- The operation and management of the public space CCTV provision, along with the process for collection, management and securing of personal data collected through this provision is registered with the Information Commissioners Office annually.
- The CCTV System is operated in compliance with the current Code of Practice issued by the Information Commissioner in respect of the operation of CCTV in public places.
- We will erect appropriate signs to notify the public of the presence of CCTV cameras and recording equipment. These signs will carry the necessary information prescribed in the Information Commissioner's Code of Practice.
- We will undertake an annual audit of CCTV practises to ensure compliance with the Data Protection Act 2018 and Information Commissioners Office (ICO) Code of Practice

Effective management of the CCTV System requires that:

- Access to all the data held, and the CCTV equipment, should comply with specific guidelines as highlighted in this code.
- The Operational Manual and documentation required to run this scheme must be developed from, and specifically linked to, this Code of Practice.

- All incidents witnessed on the CCTV System or on review of a recording will be logged.
- Data shall be stored for a maximum of 28 days before being digitally erased unless required for a specific enquiry (Flood management data will be stored for 90 days)
- All CCTV equipment will be kept in good working order and be serviced according to manufacturer recommendations.
- When a fault develops on the CCTV System, it shall be recorded on the fault management system (AMX) and the appropriate action taken to ensure a speedy repair.
- All CCTV equipment shall be secured to prevent interference from unauthorised personnel. This means that recording equipment shall be kept in a secure environment, which is a controlled and secure location.
- CCTV data shall be afforded a high level of security. Access to recordings shall be limited to Newcastleton & District Community Council appointees authorised by the Data Controller.
- All CCTV data will be stored in a secure environment to prevent unauthorised or unlawful processing of personal data and against accidental loss, damage, or destruction of personal data.

Effective management of the CCTV System requires that:

- Any data held for evidential purposes will be kept away from other personal data in a secure location.
- No unauthorised copies will be made of any personal data except with the permission of the Newcastleton & District Community Council Data Controller. They shall record the reason and ensure that all copies are numbered and that they are only disclosed to authorised parties. The Data Controller shall also ensure such personal data is not kept for longer than is necessary and is destroyed as if it were an original recording.
- No guarantee is given or implied that any incident will be observed and recorded by the System. However, all CCTV Operators and management will endeavour to provide a level of coverage based on up-to-date information concerning incidents and activities commensurate within the purposes of the CCTV System.

Cameras will not be used to view into private residential property.

Where the equipment permits it 'privacy Zones' and blackouts will be programmed into the System as required, in order to ensure that the interior of any private residential property within the range of the System is not surveyed by the cameras. All operators are fully trained in privacy issues and requirements.

It should also be acknowledged that constraints are placed upon every CCTV system by the limits of current technology.

SECTION 7 - ACCOUNTABILITY AND RESPONSIBILITIES

Newcastleton & District Community Council Authorised Appointees will have unrestricted access to the control stations and System.

The Newcastleton & District Community Council Authorised Appointees will ensure that any issues, concerns of complaint are dealt with in an appropriate and timely manner.

Newcastleton & District Community Council will have day to day responsibility for the management and maintenance of the System.

The System will be subject to regular reviews and audits.

Human resources

Newcastleton & District Community Council Authorised Appointees are fully trained in the use of the CCTV System and must adhere to the regulations and governance in place.

A regular review of SIA regulatory guidance will be undertaken.

All appointees will be provided with copies of this code and relevant documents to ensure adherence with the code and associated procedures.

Each individual (having responsibility under the terms of this code) who is involved with the system to which it refers will be subject to the organisations policies and procedures. Any breach of this code or any aspect of confidentiality will be dealt with in accordance with the relevant policy.

SECTION 8 - ACCESS AND SECURITY

Authorised Access

Only trained and authorised personnel will operate any of the equipment located within the CCTV monitoring stations, (or equipment associated with the CCTV System).

Public access

Public access to the monitoring and recording facility is restricted except for lawful, proper, and sufficient reasons and only then with the personal authority of the Newcastleton & District Community Council. Any such visits will be conducted and recorded in accordance with the Operations Manual.

Security

Authorised personnel will be always present when the equipment is in use. If the monitoring facility is to be left unattended for any reason it will be secured.

Appendix A

Supportive Information

The Information Commissioners Office (ICO)

The ICO is responsible for ensuring Data Protection Rights are observed across the United Kingdom.
The contact details for the ICO are:

Information Commissioner's Office (Scotland) 45 Melville Street, Edinburgh, EH3 7HL

Tel: 0131 244 9001

Helpline: 0303 123 1113

Email: scotland@ico.gsi.gov.uk Web site:

<https://www.ico.gov.uk/> Use of CCTV Provisions and Data Protection

Information is available to the general public on their rights at <https://ico.org.uk/for-the-public/>

Appendix B

Owner Information

Data Controller

Newcastleton District Community Council

Authorised System Owners/System Maintenance

Newcastleton District Community Council

Contact details:

secretary@newcastletoncommunitytrust.co.uk

<https://www.visitnewcastleton.com/>

This page is intentionally left blank

SELKIRK BIDS – RETENTION POLICY 30.01.23

RETENTION POLICY

1. Selkirk BIDS will ensure Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')”

Responsibility

Selkirk BIDS Data Protection Office has overall responsibility for updating members/staff on regulation changes. They will ensure everyone involved in the processing of Data is aware of the set-out retention period documentation policy.

Principles

Selkirk BIDS Data Protection Officer will ensure Selkirk BIDS follow the principles set out by the ICO on storage

- We will keep personal data for longer than we need it.
- We will consider and ensure justification for the time periods we keep personal data. This will depend on our purposes for holding the data.
- Selkirk BIDS policy sets out retention periods wherever possible, to comply with documentation requirements.
- Selkirk BIDS will periodically review the data we hold, and erase or anonymise it when we no longer need it.
- Selkirk BIDS will consider the challenges to the retention of data. Individuals have a right to erasure if we no longer need the data.
- Selkirk BIDS will clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.

SELKIRK BIDS – RETENTION POLICY 30.01.23

TYPES OF DATA STORED

This Policy applies to all official records generated in the course of the Selkirk BIDS operations, including but not limited to:

- Typed, or printed hardcopy (i.e., paper) documents
- Electronic records and documents (e.g., email, Web files, text files, PDF files)
- Video or digital images
- Graphic representations
- Electronically stored information contained on network servers and/or document management systems
- Recorded audio material

FURTHER HELP AND ADVICE

For more information and advice about this policy contact

Data Protection Officer

Selkirk BIDS

48 High Street

Selkirk

TD7 4DD

Email: DAVCANDERSON@AOL.COM

Web: <https://www.exploreselkirk.co.uk>

ICO Scotland contact details

The Information Commissioner's Office – Scotland

Queen Elizabeth House

Sibbald Walk

Edinburgh

EH8 8FT

Telephone: 0303 123 1115

Email: Scotland@ico.org.uk

**SELKIRK BIDS –
RETENTION POLICY 30.01.23**

Guidelines for data retention within Selkirk BIDS

<u>Grouping Type</u>	<u>Type of data we may hold</u>	<u>Suggested retention period</u>
Staff	Personnel records	7 years from end of employment
	Salary & payroll	7 years
	Pensions documents	Permanently
Charities	Quarterly reviews and charity/fund information	Longer of 3 years from the end of the fund or to meet the Grant letter requirements.
Board of Directors	Contact details, Register of Interests & expense claims	7 years from end of Trusteeship
Investors & donors	Basic contact data & award letters*	10 years after last donation
Volunteer Members	Basic contact details	1 year from last contact
	CV's where appropriate	
Prospective employees not offered a position	CVs	2 years
	Interview records	
Service Users	Contact details Income, Salary and employment details Health information Energy Bills GP contact details Education Bank Details	7 years after service
CCTV	Digital images	Period of 28 days unless required for a specific enquiry

**SELKIRK BIDS –
RETENTION POLICY 30.01.23**

Data protection impact assessments

guidance for carrying out a data protection impact assessment on surveillance camera systems

Introduction: a collaborative approach

1. The Surveillance Camera Commissioner (SCC) and the Information Commissioner's Office (ICO) have worked together on this guidance. By doing this we've responded to requests from operators of surveillance camera systems who have asked for coordinated advice when processing personal data in this way. The template we've provided should support you through the process, but you may prefer to use alternatives. It is perfectly acceptable to do this, provided that they satisfy statutory requirements (see legal obligations set out below).

The roles of the Commissioners

2. The SCC is responsible for encouraging relevant authorities¹ to be compliant with the [Home Secretary's Surveillance Camera Code of Practice](#); to review the operation of the code and to provide advice about it. Relevant authorities in England and Wales are required to have due regard to the code when they are operating surveillance cameras, as defined at section 29(6) of the Protection of Freedoms Act 2012, in public places. The SCC also has a statutory responsibility to encourage voluntary adoption of the code by organisations not listed in the Act.
3. The ICO is responsible for regulating and enforcing data protection law, namely the General Data Protection Regulation and the Data Protection Act 2018.² It has published [detailed guidance](#) on data protection impact assessments (DPIAs), for general processing and for the law enforcement purposes, which you should read in conjunction with this advice. All organisations in the UK must comply with data protection law, and in certain cases, carrying out a DPIA is a mandatory requirement.

Who is this advice for?

4. This advice is intended for organisations in England and Wales that must have regard to the Surveillance Camera Code of Practice under Section 33(5) of the Protection of Freedoms Act 2012. However, it will also be of value to the wider community of public authorities and any other bodies, whether public or private, who perform public functions as well as private organisations operating surveillance cameras anywhere in the UK.
5. When considering the deployment of a surveillance camera system, you must have a clear understanding of each organisation's responsibilities under data protection law. If you are making decisions on the use of the personal data captured as a controller, or joint controllers, you are chiefly responsible for compliance with data protection law, including the requirement to carry out a DPIA. However, other organisations acting under the instruction of controllers (i.e. processors) also have responsibilities, including assisting controllers in developing DPIAs.
6. If you then process this data for different purposes, you will also need to consider these in any assessment. In some cases, if the processing is for different purposes, you may be required to carry out more than one DPIA.

Your legal obligations

7. Principle 2 of the Surveillance Camera Code of Practice³ states that the use of a surveillance camera system must take into account its effect on individuals and their privacy. Processing of

¹ Listed in the [Protection of Freedoms Act 2012 \(s33.5\)](#) – police forces, police and crime commissioners, local authorities and parish and district councils.

² Regulation (EU) 2016/679 of the European Parliament and European Council, also known as the General Data Protection Regulation, was transposed into UK law through the Data Protection Act 2018. Any processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences is regulated under Part 3 of the Data Protection Act 2018 which transposes Directive (EU) 2016/680, also known as the Law Enforcement Directive, into UK law.

³ Surveillance Camera Code of Practice issued by the Home Secretary in June 2013 under Section 30(1)(a) Protection of Freedoms Act 2012.

personal data using a surveillance camera system will be considered 'likely to result in high risk to rights and freedoms' under data protection law. For instance, where it can systematically monitor public spaces on a large scale, or can involve innovative technology or the processing of biometric data. As processing using a surveillance camera system is likely to be high risk you must conduct a DPIA **before** the system is installed and review it regularly. Carrying out a DPIA means that you can determine whether deployment is lawful, and will also be a record of how you have considered and addressed any risks or wider concerns about your project. This addresses Principle 2 of the Surveillance Camera Code of Practice as well as requirements of data protection law.

8. What a DPIA must cover and when they are required by law is set out in Article 35 of the GDPR (general processing) and Section 64 DPA 2018 (law enforcement processing). **The ICO has also identified further types of general processing where a DPIA is mandatory, because the processing is likely to result in high risk⁴ to individuals' rights and freedoms.** This can also indicate to controllers who are processing for law enforcement purposes where there may be high risk. Surveillance camera systems are very likely to sit within the scope of this high risk requirement.
9. There are situations when you must consider a DPIA, for example:
 - When you are introducing a new surveillance camera system.
 - Before you process any special categories of personal data on a large scale.
 - If you are considering introducing new or additional technology that may affect individuals' rights and freedoms (e.g. facial recognition technology, automatic number plate recognition (ANPR), audio recording, body worn cameras, unmanned aerial vehicles (drones), megapixel or multi sensor very high-resolution cameras).
 - If your system involves any form of data matching.
 - When you are changing the location or field of view of a camera or other such change that may raise privacy concerns.
 - When you are reviewing your system to ensure that it is still justified. Both the SCC and the ICO recommend that you review your systems regularly, for example as part of annual procedures.
 - When you change the way you record images and handle, use or disclose information.
 - When you increase the geographical area captured by your surveillance camera system.
 - When you change or add an end user or recipient for the recorded information or information derived from it.

Remember that the ICO has identified **specific circumstances** when a DPIA is required.

Assessing risk

10. Likelihood of high risk means that the type of processing has a higher chance of harming individuals. This could be as a result of decisions taken using this data, or because of an individual's lack of control over how their information is used. 'Likely' does not mean that your project **will** harm individuals, however it does mean that you are required to assess your project before it starts, to ensure you reduce any risks you identify.
11. The GDPR identifies certain types of processing where the likelihood of high risk is engaged, for example stating specifically that a DPIA "shall in particular be required in the case of...systematic monitoring of publicly accessible places on a large scale" (Article 35).

⁴ Examples of high risk could be surveillance cameras, such as body worn video, that also record audio or CCTV fitted with automatic facial recognition capabilities. There is further information about when to carry out a DPIA on the ICO website.

12. To assess the level of risk, you must consider both the **likelihood** and the **severity** of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm. It is important to embed DPIAs into your organisational processes such as project planning and other management and review activities, and ensure the outcome can influence your plans prior to implementation.
13. A further benefit of carrying out a DPIA is that it will help to address statutory requirements under the Human Rights Act 1998 (HRA). Section 6(1) HRA provides that it is unlawful for a public authority to act in a way which is contrary to the rights guaranteed by the European Convention on Human Rights (ECHR). Therefore, in addition to the above, as a public body or any other body that performs public functions you must make sure that your system complies with HRA requirements.
14. When conducting a DPIA you should consider the nature, scope, context and purposes of the surveillance camera activities and their potential to interfere with the rights and freedoms of individuals, as set out in Human Rights law. For example:
 - the right to freedom of assembly;
 - freedom of thought, belief and religion;
 - freedom of expression;
 - freedom of association; and
 - the protection from discrimination in respect of those rights and freedoms.
15. Data controllers should consider how the processing is lawful and fair, in order to be compliant with the first principle of data protection law.
16. If your DPIA identifies a residual high risk that you cannot mitigate adequately, data protection law requires that you must **consult the ICO** before starting to process personal data. This should be when you are planning your surveillance camera system or making changes to it that will impact on individuals' rights and freedoms.
17. To support you in preparing your assessment the accompanying template includes:
 - **DPIA** to describe and assess your planned deployment of surveillance cameras;
 - **Appendix One** to record and evaluate your camera locations, equipment and software;
 - **Appendix Two** with suggested steps involved in carrying out a DPIA; and
 - **Appendix Three** a sample risk matrix.

Governance of DPIAs

18. You must carry out a DPIA prior to the processing in the first instance. If the deployment goes ahead, you should review the DPIA regularly to maintain relevance. You should be aware that failure to complete a DPIA prior to the deployment of a surveillance camera system could result in the ICO taking enforcement action.
19. As an organisation that operates a surveillance camera system you will also be the controller of the personal data captured by its cameras. Under DPA 2018 (Sections 69-71), a data controller is under a legal obligation to designate and resource a data protection officer and to seek their advice when carrying out a DPIA.
20. Consultation is an important part of the DPIA process. You should obtain the views of people who are likely to come under surveillance or their representatives. This can often be achieved by existing local consultation mechanisms such as local area committees or safer neighbourhood team meetings. You can consider other methods, such as face to face interviews, online surveys,

and addressing focus groups, crime and disorder partnerships and community forums. You should also consult internally, for example with your legal department, and staff who will be recorded. Your DPO may be able to offer advice on how to carry out consultation. The Surveillance Camera Commissioner's [Passport to Compliance](#) (paragraph 1.5.3) also includes detailed advice on consultation which will be of use.

21. Principle 2 of the Surveillance Camera Code of Practice also requires that you must carry out regular reviews to ensure your use of surveillance camera systems remains justified. You should factor a review of your DPIA into your ongoing risk assessment procedures to consider any significant changes to the risks of operating an existing system (for example extended access to footage to additional parties, or changing the location or capabilities of the system).

DPIA Template

22. The questions in the DPIA will enable you to determine:

- Are surveillance cameras the right solution to the problem you are trying to solve?
- What are the risks to data subjects raised by the deployment of surveillance cameras?
- Is the impact on individuals' rights and freedoms proportionate to the problem you are addressing?
- Can the risks be reduced to an acceptable level?

The tools at Appendix Two and Three may also assist you to do this.

Appendix One

23. When undertaking a DPIA, it is important to be able to identify where your cameras are located. It is good practice to maintain an asset register for all of your hardware (including cameras), software and firmware. This allows the system operator to record each site and system component of a surveillance camera system.
24. The template at Appendix One is designed to give you a clear and systematic format for recording camera locations, other hardware, software and firmware on your surveillance camera system, and demonstrate the mitigations of risk particular to specific camera locations and functionality.
25. This approach allows you to document a generic and methodical approach to any intrusion into privacy, catalogue your cameras by type and location, and identify specific privacy risks with particular cameras.
26. If any new site or installation sits outside of the pre-defined fields, or additional integrated surveillance technologies are added, then you can add new categories as required.

Appendix Two demonstrates suggested steps in the lifecycle of a DPIA.

Appendix Three shows an example of a risk assessment matrix.

This page is intentionally left blank



**SURVEILLANCE CAMERA
COMMISSIONER**

ico.
Information Commissioner's Office

Data protection impact assessments template for carrying out a data protection impact assessment on surveillance camera systems

Project name: SELKIRK BIDS

Data controller(s): DAVID ANDERSON

This DPIA template should be completed with reference to the guidance provided by the Surveillance Camera Commissioner and the ICO. It will help you to identify whether the use of surveillance cameras is appropriate for the problem you wish to address, assess the risks attached to your project and form a record of your decision making.

1. Identify why your deployment of surveillance cameras requires a DPIA¹:

¹ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/>

- | | |
|---|---|
| <input type="checkbox"/> Systematic & extensive profiling | <input type="checkbox"/> Large scale use of sensitive data |
| <input type="checkbox"/> Public monitoring | <input type="checkbox"/> Innovative technology |
| <input type="checkbox"/> Denial of service | <input type="checkbox"/> Biometrics |
| <input type="checkbox"/> Data matching | <input type="checkbox"/> Invisible processing |
| <input type="checkbox"/> Tracking | <input type="checkbox"/> Targeting children / vulnerable adults |
| <input type="checkbox"/> Risk of harm | <input type="checkbox"/> Special category / criminal offence data |
| <input type="checkbox"/> Automated decision-making | <input type="checkbox"/> Other (please specify) |

2. What are the timescales and status of your surveillance camera deployment? Is this a proposal for a new deployment, or the expansion of an existing surveillance camera system? Which data protection regime will you be processing under (i.e. DPA 2018 or the GDPR)?

Describe the processing

3. Where do you need to use a surveillance camera system and what are you trying to achieve? Set out the **context** and **purposes** of the proposed surveillance cameras or the reasons for expanding an existing system. Provide evidence, where possible, including for example: crime statistics over an appropriate time period; housing and community issues, etc.

4. Whose personal data will you be processing, and over what area? Set out the **nature** and **scope** of the personal data you will be processing. Who are the data subjects, and what kind of information will you be collecting about them? Do they include children or vulnerable groups, and what is the scale and duration of the processing?

5. Who will be making decisions about the uses of the system and which other parties are likely to be involved? Will you be the sole user of the data being processed or will you be sharing it with other organisations or agencies? Record any other parties you would disclose the data to, for what purposes, and any relevant data sharing agreements. Note that if you are processing for more than one purpose you may need to conduct separate DPIAs.

6. How is information collected? (tick multiple options if necessary)

- | | |
|---|---|
| <input type="checkbox"/> Fixed CCTV (networked) | <input type="checkbox"/> Body Worn Video |
| <input type="checkbox"/> ANPR | <input type="checkbox"/> Unmanned aerial systems (drones) |
| <input type="checkbox"/> Stand-alone cameras | <input type="checkbox"/> Redeployable CCTV |
| <input type="checkbox"/> Other (please specify) | |

7. Set out the information flow, from initial capture to eventual destruction. You may want to insert or attach a diagram. Indicate whether it will include audio data; the form of transmission; the presence of live monitoring or use of watchlists; whether data will be recorded; whether any integrated surveillance technologies such as automatic facial recognition are used; if there is auto deletion after the retention period. You may have additional points to add that affect the assessment.

8. Does the system’s technology enable recording?

- Yes No

If recording is enabled, state where it is undertaken (no need to stipulate address, just Local Authority CCTV Control room or on-site will suffice for stand-alone camera or BWV), and whether it also enables audio recording.

9. If data is being disclosed, how will this be done?

- Only by on-site visiting
- Copies of footage released (detail method below, e.g. encrypted digital media, via courier, etc)
- Off-site from remote server
- Other (please specify)

10. How is the information used? (tick multiple options if necessary)

- Monitored in real time to detect and respond to unlawful activities
- Monitored in real time to track suspicious persons/activity
- Compared with reference data of persons of interest through processing of biometric data, such as facial recognition.
- Compared with reference data for vehicles of interest through Automatic Number Plate Recognition software
- Linked to sensor technology
- Used to search for vulnerable persons
- Used to search for wanted persons
- Recorded data disclosed to authorised agencies to support post incident investigation, including law enforcement agencies
- Recorded data disclosed to authorised agencies to provide intelligence
- Other (please specify)

Consultation

11. Record the stakeholders and data subjects you have consulted about the deployment, together with the outcomes of your engagement.

Stakeholder consulted	Consultation method	Views raised	Measures taken

Consider necessity and proportionality

12. What is your lawful basis for using the surveillance camera system? Explain the rationale for your chosen lawful basis under the relevant data protection legislation. Consider whether you will be processing special categories of data.

13. How will you inform people that they are under surveillance and ensure that they are provided with relevant information? State what privacy notices will be made available and your approach to making more detailed information available. Consider whether data subjects would reasonably expect to be under surveillance in this context.

14. How will you ensure that the surveillance is limited to its lawful purposes and the minimum data that is necessary for those purposes? Explain the adequacy and relevance of the data you will be processing and how it is limited to the purposes for which the surveillance camera system will be deployed. How will you know if it is delivering the benefits it has been deployed for?

15. How long is data stored? (please state and explain the retention period)

16. Retention Procedure

- Data automatically deleted after retention period
- System operator required to initiate deletion
- Under certain circumstances authorised persons may override the retention period, e.g. retained for prosecution agency (please explain your procedure)

17. How will you ensure the security and integrity of the data? How is the data processed in a manner that ensures appropriate security, protection against unauthorised or unlawful processing and against accidental loss, destruction or damage? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

18. How will you respond to any subject access requests, the exercise of any other rights of data subjects, complaints or requests for information? Explain how you will provide for relevant data subject rights conferred under the legislation. You must have procedures in place to respond to requests for camera footage in which a subject appears, and to respond to any other request to meet data protection rights and obligations.

19. What other less intrusive solutions have been considered? You need to consider other options prior to any decision to use surveillance camera systems. For example, could better lighting or improved physical security measures adequately mitigate the risk? Does the camera operation need to be continuous? Where you have considered alternative approaches, provide your reasons for not relying on them and opting to use surveillance cameras as specified.

20. Is there a written policy specifying the following? (tick multiple boxes if applicable)

- The agencies that are granted access
- How information is disclosed
- How information is handled

Are these procedures made public? Yes No

Are there auditing mechanisms? Yes No

If so, please specify what is audited and how often (e.g. disclosure, production, accessed, handled, received, stored information)

Identify the risks

Identify and evaluate the inherent risks to the rights and freedoms of individuals relating to this surveillance camera system. Consider, for example, how long will recordings be retained? Will they be shared? What are the expectations of those under surveillance and impact on their behaviour, level of intrusion into their lives, effects on privacy if safeguards are not effective? Could it interfere with other human rights and freedoms such as those of conscience and religion, expression or association. Is there a risk of function creep? Assess both the likelihood and the severity of any impact on individuals.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Address the risks

Explain how the effects of privacy enhancing techniques and other features mitigate the risks you have identified. For example, have you considered earlier deletion of data or data minimisation processes, has consideration been given to the use of technical measures to limit the acquisition of images, such as privacy masking on cameras that overlook residential properties? What security features, safeguards and training will be in place to reduce any risks to data subjects. Make an assessment of residual levels of risk.

Note that APPENDIX ONE allows you to record mitigations and safeguards particular to specific camera locations and functionality.

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk			
Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved?
	Eliminated reduced accepted	Low medium high	Yes/no

Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved?
	Eliminated reduced accepted	Low medium high	Yes/no

Authorisation

If you have not been able to mitigate the risk then you will need to submit the DPIA to the ICO for prior consultation. [Further information](#) is on the ICO website.

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by:		If you identify a high risk that you cannot mitigate adequately, you must consult the ICO before starting to capture and process images.
DPO advice provided by:		DPO should advise on compliance and whether processing can proceed.
Summary of DPO advice		
DPO advice accepted or overruled by: (specify role/title)		If overruled, you must explain your reasons.
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons.
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA.

APPENDIX ONE

This template will help you to record the location and scope of your surveillance camera system and the steps you've taken to mitigate risks particular to each location.

Location: Each system operator/owner should list and categorise the different areas covered by surveillance on their system. Examples are provided below.

Location type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
Town centre	All	250	24hrs	24hrs (only maximum 3 operators) – likely average patrol high hourly	The privacy level expectation in a town centre is very low; our town centres are well signed with appropriate signage for CCTV its use and purpose with contact details.
Public car park	1, 5, 6	100			
Parks					HD camera only include due to proximity to town HD cam
Play areas					
Housing blocks internal	1, 2	200	24hrs (calendar month)	Limited due to the fact that most are static cameras	High level asb historical problems (please see statistical assessment in annual review)
Housing estate (street)					
Residential street					Cameras are installed here to respond to high crime trends, deal with the fear of crime

APPENDIX TWO: STEPS IN CARRYING OUT A DPIA



APPENDIX THREE: DATA PROTECTION RISK ASSESSMENT MATRIX

Use this risk matrix to determine your score. This will highlight the risk factors associated with each site or functionality.

Matrix Example:

	Camera Types (low number low impact – High number, High Impact)									
	→									
Location										
Types										
A (low impact)										
Z (high impact)										

NOTES

SELKIRK BIDS – SECURITY POLICY 30.01.23

SECURITY

A key principle of the UK GDPR is that Selkirk BIDS processed personal data securely by means of ‘appropriate technical and organisational measures’ – this is the ‘security principle’.

- Selkirk BIDS will undertake risk analysis, implement organisational policies, and ensure physical and technical measures are in place to support the security policy. When implementing our policies, we have taken into account the additional requirements about the security of our processing – and these also apply to those who process data in line with Selkirk BIDS activities. All nominated staff accessing CCTV will be Disclosure Checked in accordance with current Legislation.
- Selkirk BIDS will undertake and review annually analysis (or sooner if the need arises) of the risks presented by our processing and use this to assess the appropriate level of security we need to put in place, and to improve our policies where possible.
- When deciding what measures to implement, we take account of the state of the art and costs of implementation.
- Selkirk BIDS have taken steps to implement our Security Policy and we have additional policies including training, code of conduct, privacy policies in place to enforce them. These policies have been assessed by Selkirk BIDS, and what we need to do by considering the security outcomes we want to achieve. We have put in place basic technical controls such as those specified by established frameworks like Cyber Essentials.
- We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process. We use encryption in our communication where it is appropriate to do so.
- Selkirk BIDS has policies in place which covers requirements of confidentiality, integrity and availability for the personal data we process. We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.
- Selkirk BIDS conducts regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement. Where appropriate, we implement measures that adhere to our code of conduct. We ensure that any data processor we use also implements appropriate technical and organisational measures.

SELKIRK BIDS – SECURITY POLICY 30.01.23

FURTHER HELP AND ADVICE

For more information and advice about this policy contact

Data Protection Officer

Selkirk BIDS

48 High Street

SELKIRK

TD7 4DD

Email: DAVCANDERSON@AOL.COM

Web: <https://www.exploreselkirk.co.uk>

ICO Scotland contact details

The Information Commissioner's Office – Scotland

Queen Elizabeth House

Sibbald Walk

Edinburgh

EH8 8FT

Telephone: 0303 123 1115

Email: Scotland@ico.org.uk

SELKIRK BIDS

DATA PROTECTION TRAINING POLICY – 30.01.23

Introduction

Selkirk BIDS recognised that everyone has rights in regards of the way in which their personal data is handled.

During the course of Selkirk BIDS activities we will collect, store and process personal Data.

We recognise that the correct and lawful treatment of this personal data will maintain confidence in the organisation and will provide for successful operations.

1. Responsibility

The responsibility for the production and maintenance of this document is with the Data Protection Officer as detailed within the Privacy policy. They will also ensure that any substantive changes made will be communicated to all relevant personnel.

2 Volunteer /Staff Data Protection Training Policy

Selkirk BIDS Data Protection Training Policy is the responsibility of the Data Protection Officer to ensure that the policy set is and remains internally consistent.

It is the responsibility of the Data Protection Officer ensure that Data Protection training is provided to all new volunteers/employees as part of their induction program and volunteers/employees are provided with regular refresher training to include any updates or changes.

3 Scope

This policy applies to all volunteers, permanent, temporary or contracted employees of Selkirk BIDS who are able to access information.

4 Purpose and Objectives

The purpose and objectives of this policy are in addition to those fully detailed within Selkirk BIDS Privacy Policy and CCTV Codes of Practice.

The purpose of this policy is to set out the training that staff will be provided with to ensure that all handling of personal data is compliant with UK data protection legislation (including GDPR).

5. Frequency of Training

Training required by this policy should be provided to all new volunteers/employees as part of their induction program.

All existing volunteers/employees shall also be provided with the training required by this policy unless this has been provided to them already.

All volunteers/employees shall receive a refresher of relevant training at least every twelve months or following a material change in data protection law or regulation.

Selkirk BIDS will keep a record of what training has been undertaken by each data user.

SELKIRK BIDS DATA PROTECTION TRAINING POLICY – 30.01.23

6. Training for Data Users

All volunteers/employees will receive training on their responsibilities under Selkirk BIDS Privacy and CCTV Codes of Practice and all of its listed sub-policies and supporting procedures. All nominated staff will be Disclosure Checked in accordance with current Legislation.

This will include guidance on:

Data Protection Principles:

- what data processing is;
- how personal data must be handled in accordance with the data protection principles;
- awareness that failure to comply with the information governance requirements contained in NDCC policies may result in disciplinary action; and
- the possibility that they may commit criminal offences if they deliberately try to access, or to disclose, personal data without authority.

Day to day office security:

- personal desk and work area management;
- implementation of the company's Clear Desk, Clear Screen Policy;
- the disposal of confidential waste;
- password management and the company's Password Policy;
- how to access and exit the premises;
- visitor security and management; and
- the use of portable media and cloud-based storage facilities.

Data Breach and Incident Reporting:

- how to identify a possible data breach;
- how suspected and actual security breaches affecting our systems should be dealt with; and
- how to report a possible data breach and comply with the company's

Incident Reporting Policy.

Additional training for those responsible for handling actual or suspected security breaches will include reference to any guidance from the ICO on the handling of data security breaches and the notification of such breaches to the ICO.

Email usage and document protection:

- how all employees should use email;
- where when and how encrypted email should be used;
- understanding the difference between encryption and password protection.

SELKIRK BIDS DATA PROTECTION TRAINING POLICY – 30.01.23

Data subject access requests:

- understanding what a Subject Access Request (SAR) is; and Staff Data Protection Training Policy
- what action needs to be taken when a SAR is received.

Additional training will be provided to those at Selkirk BIDS who are responsible for accepting instructions from our clients. Such training will include:

- understanding the lawful reasons for undertaking an investigation;
- the purposes for which personal data can be processed;
- the purposes for which sensitive personal data can be processed;
- what considerations must be taken into account when planning an investigation;
- understanding why and where privacy impact assessments must be undertaken;
- how to undertake a Privacy Impact Assessment;
- awareness of the need to check an individual's identity before providing them with personal data and undertake due diligence;
- the dangers of individuals attempting to obtain or alter personal data by deception;
- other issues that data users should be aware of in relation to data held in relation to the investigations and assignments we undertake; and
- the importance of raising any queries or concerns about the processing of personal data with NDCC Data Protection Officer.

Additional training will be provided to those at Selkirk BIDS who are responsible for marketing and our customer newsletters, this additional training will include:

- what personal data Selkirk BIDS process;
- what consent is required to email a potential customer;
- how to obtain consent;
- when and how privacy notices need to be provided to data subjects; and
- what information should be included in a privacy notice.

Additional training will be provided to those at Selkirk BIDS who are responsible for advising about compliance with employment law obligations or personnel management. The content of such training will be determined by the Board following consultation with the Data Protection Officer

FURTHER HELP AND ADVICE

For more information and advice about this policy contact

Data Protection Officer

Selkirk BIDS

48 High Street

SELKIRK

TD7 4DD

Email: DAVCANDERSON@AOL.com

Web: <https://www.exploreselkirk.co.uk>

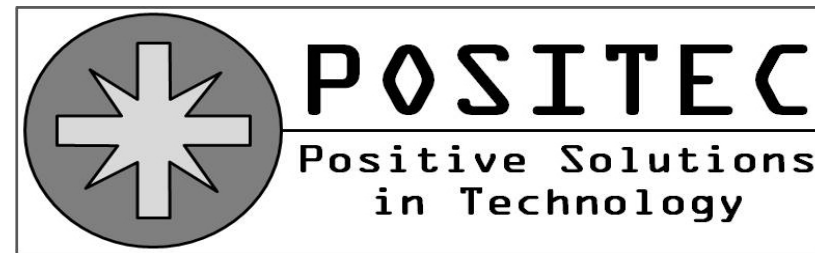
SELKIRK BIDS
DATA PROTECTION TRAINING POLICY – 30.01.23

ICO Scotland contact details

The Information Commissioner's Office – Scotland
Queen Elizabeth House
Sibbald Walk
Edinburgh
EH8 8FT
Telephone: 0303 123 1115
Email: Scotland@ico.org.uk

Selkirk Town Ctr – HD CCTV solution

Page 165



In partnership with



Positec (UK) Ltd – 19/12/22

Peter Stanhope - 07778 514150

peter.stanhope@positec-ltd.com

Selkirk Town Ctr – HD CCTV solution

Page 166



Project Scope

- To review the current CCTV solution (5 locations) within the town centre of Selkirk,
- Identify the locations that require coverage based on business needs,
- Produce a solution based on the technical solution already in place at Alloa Town Centre plus numerous other locations,
- Identify where the core equipment (Network Video Recorder – NVR) and other key components will be housed,
- Identify the items that will need to be actioned by the local community,
- Carry out client sponsored survey on 20th Dec 2019.
- Site review on 25th November 2021
- Pricing review 19th December 2022 based on planning permission design.

Positec (UK) Ltd – 19/12/22

Peter Stanhope - 07778 514150

peter.stanhope@positec-ltd.com

Selkirk Town Ctr – HD CCTV solution


During the survey on the 20th Dec 2019 the following was identified as the business requirements, then updated on 25th Nov. '21.....

- 1 CCTV locations, BLUE important
- W Revised location for NVR & Internet connection – D Anderson Office

↔ Very high speed radio links

↔ High speed radio link (dotted only if access needed at Police station)





POSITEC
Positive Solutions
in Technology

HD CCTV & Networking Solutions

Peter Stanhope
07778 514150
peter.stanhope@positec-ltd.com

19/12/2021

Project Selkirk Community CCTV solution

No	Number	Location	Description	Diver		PI2	Budget	M0	F000
				Many	Switch				
Core	W	David Anderson Office	NVR to be located there	1	1				
1	1	Mungo Park	Using existing pole, radio to Loc2	1	1		1	1	
2	2	Bottom Tower St	High speed link to Loc1	1	1	1	1	1	
3	3	Market Place pole	LOS feed from Loc2	1	1	1	1	1	
4	4	Above level	LOS feed from Loc3	1	1		1	1	
5	5	Top Tower St	Primary radio link to VNI, plus to bottom tower St	1	1		1	1	
6	6	Post Office	Needed for LOS link to Loc2	1	1			1	
7	7	ScotNet	For LOS link to Loc6 and onwards to Loc8	1	1		1	1	
8	8	Near Memorial Park	LOS link to ScotNet	1	1		1	1	0
Sub total						2	12	8	0

Positec (UK) Ltd – 19/12/22
Peter Stanhope - 07778 514150
peter.stanhope@positec-ltd.com

Selkirk Town Ctr – HD CCTV solution



The solution on the previous page provides....

- A 'turn key solution' - so only input from the client is as per below once final design is concluded,
- Remote access/viewing will be possible if Internet access is made available,
- Networking equipment to be located in D Anderson office, or any other location with access to the LOS radio links, plus Internet access.

Client responsibility

- Arrange with SBC for permission to use the existing CCTV poles, gain access to the base of the locations at 1 to 5, plus equipment in the office and on the roof of Victoria Hall,
- Cherry picker or similar high access vehicle during the on site implementation,
- A permanent mains point at all locations, current and new, could be with SBC for permission to use the 'festive' power source around the town centre if required
- Arrange with ScotBet for permission to place equipment on their building,
- Arrange with Post Office for permission to place equipment on their building,
- Internet access & NVR located in D Anderson Office.

Positec (UK) Ltd – 19/12/22

Peter Stanhope - 07778 514150

peter.stanhope@positec-ltd.com

Selkirk Town Ctr – HD CCTV solution v4

Page 169



Costing.

The solution is based on

- High speed radio links between the locations identified on the left,
- HD CCTV cameras as listed on page 3 with a 64ch NVR located at W,
- A 'turn key solution' with all equipment owned by Selkirk Town Ctr,
- Payment terms, 50% on placement of order, final payment within one week of work completed and invoiced.
- One year warranty for all equipment supplied,
- Remote access/viewing will be available if Internet access is made available.

Radio infrastructure	- £10.7K
CCTV & NVR	- £18.9K
Total expenditure	- £29.6K + VAT

Annual running costs

CCTV/Radio	- £ unknown, depending on business needs
Internet access	- £ unknown, depending on solution

Positec (UK) Ltd – 19/12/22
Peter Stanhope - 07778 514150
peter.stanhope@positec-ltd.com

HD CCTV solution components

Fixed lens camera

- High quality optical lens providing coverage to a specific area,
- Based on client requirements, can be 'zoomed in' or on 'wide angle' during installation,
- Night time Infra Red (IR) automatically activated,
- Customisable name and time on the video feed.



← Daytime viewing



← Automatic 'black and white' when light levels dictate.

NOTE High resolution pictures on monitor and recordings. Pictures not representative.

Positec (UK) Ltd – 20/12/19

Peter Stanhope - 07778 514150

peter.stanhope@positec-ltd.com

180 degree camera

- Used to cover a relatively wide area,
- New to the market,
- Can be setup to give very little 'blind spot' below the camera,
- Very high resolution, fixed lens and position,
- Customisable name and time on the video feed.



Daytime viewing



Automatic 'black and white' when light levels dictate.

NOTE High resolution pictures on monitor and recordings. Pictures not representative.

Positec (UK) Ltd – 20/12/19

Peter Stanhope - 07778 514150

peter.stanhope@positec-ltd.com

Fisheye camera



- Ultra high resolution to cover a compact area close to camera location,
- New to market providing 360 degree coverage from one camera,
- Can be setup to give no blind spot below the camera,
- Powerful IR array for excellent night viewing,
- Customisable viewing positions, high Megapixel, fixed lens,
- Customisable name and time on the video feed.

Daytime viewing



Automatic 'black and white' when light levels dictate.

NOTE High resolution pictures on monitor and recordings. Pictures not representative.

Positec (UK) Ltd – 20/12/19

Peter Stanhope - 07778 514150

peter.stanhope@positec-ltd.com

Pan Tilt Zoom (PTZ) camera



- HD Pan Tilt Zoom (PTZ) cameras are available in many forms,
- Used to cover a relatively wide area,
- Optical lens often from 10x to 36x zoom,
- Presets setup by the client to cover required views,
- Powerful IR for night time illumination, variable IR depending on zoom status,
- Customisable name and time on the video feed.

Night time viewing



Automatic 'black and white' when light levels dictate.

NOTE High resolution pictures on monitor and recordings. Pictures not representative.

Positec (UK) Ltd – 20/12/19

Peter Stanhope - 07778 514150

peter.stanhope@positec-ltd.com

Remote viewing – via the Internet



- Core of a solution is the Network Video Recorder (NVR) which is accessed for remote viewing,
- An NVR capacity typically varies between 9 and 64 channels (cameras)
- Storage capacity is sized based on client requirements – number of cameras and ‘estimate’ of days storage needed,
- With Internet access at the NVR location, and correct security settings, then remote viewing is possible over the Internet, via WiFi or 4G access,
- Software available for Android and Apple devices on client supplied hardware,
- Customisable screen layout per user.

Daytime viewing



Automatic ‘black and white’ when light levels dictate.

NOTE High resolution pictures on monitor and recordings. Pictures not representative.

Positec (UK) Ltd – 20/12/19

Peter Stanhope - 07778 514150

peter.stanhope@positec-ltd.com

HD CCTV solution components



Fisheye camera

- providing 360 degree coverage over area directly below.
- Disc shaped approx. 200mm diameter by 50mm thick – similar to smoke detector,
- Single cable installation with POE power solution.

Pan Tilt Zoom

- A Pan Tilt Zoom (PTZ) camera is controlled remotely, provides 360 degree rotation & 90 degree vertical,
- Optical zoom of usually 10x magnification.
- Size of dome approx. 250mm, total height 350mm and offset from wall 350mm,
- Single cable installation with POE+ power solution.

Bullet Camera

Fixed viewing at installation,
Approx 80mm diameter and 250mm length

Radio link

Directional antenna approx. 250mm tall, 80mm wide and 50mm thick.
Powered over Cat5e cable from local POE Ethernet switch

180degree camera

Shorter than a bullet, but slightly 'fatter'
Size approx. 200mm long by 100mm diameter

NOTE

All cameras are Power Over Ethernet (POE) so single Cat5e external grade cable to each location from Pole/cabinet where the POE Switch will require 240V dedicated power.

Cameras go automatic into 'black and white' when light levels dictate, Night time Infra Red (IR) automatically activated.

SELKIRK BIDS – PUBLIC CCTV DOCUMENTATION

INDEX

Section 1

Copy of Planning Application from SBC

Section 2

Selkirk BIDS CCTV – Landowner Permission List

Section 3

a Selkirk BIDS CCTV – Privacy Notice

b Selkirk BIDS CCTV – Code of Practice

b Selkirk BIDS CCTV – Access Permissions

c Selkirk BIDS CCTV Procedures – To Support Information Security Policy Framework

Section 4

Selkirk BIDS CCTV – Data Protection Register

Section 5

a Selkirk BIDS CCTV – ICO Data Protection Impact Assessments completed

b Selkirk BIDS CCTV – Access Policy

c Selkirk BIDS CCTV – Training Policy

d Selkirk BIDS CCTV – Security Policy

e Selkirk BIDS CCTV – Retention Policy

f Selkirk BIDS CCTV – Destruction Policy

g Selkirk BIDS CCTV – Data Protection Complaints Policy

This page is intentionally left blank

SELKIRK BIDS

CCTV PRIVACY NOTICE 30.01.23

Introduction

This privacy notice explains how Selkirk BIDS uses your data when captured on CCTV. Selkirk BIDS has CCTV in operation at various locations in and strategic points around Selkirk. CCTV will capture images in real time wherever the cameras are pointed. These cameras may capture footage of you whilst you are in and around areas of Selkirk. These Cameras have been situated outside of buildings and in public spaces and signs are in place to inform you where cameras are in use.

Who will be using your data?

Selkirk BIDS will be the data controller for the data you provide to us.

What personal data do we use?

- Static and moving images of people
- Vehicle registration numbers

What types of special category personal data do we need from you?

We do not deliberately set out to capture any special category personal data. However, cameras may incidentally record information which falls within these categories. Additionally, footage cameras may be used as evidence regarding criminal offences or related security measures.

Why do we use your data?

- To ensure the safety of residents and visitors
- To detect, prevent or reduce the incidence of crime
- To reduce the fear of crime
- To create a safer environment
- To capture and record river levels for flood recording purposes

What legal reasons allow us to use your data in this way?

Our legal basis for processing your personal data is:

- That it is necessary to meet a legal obligation
- That it is necessary to perform tasks in the public interest
- That we have a legitimate interest in processing this information

Our basis for processing special category personal data is:

There is a substantial public interest in processing this information, for the purposes of detecting and preventing crime

SELKIRK BIDS

CCTV PRIVACY NOTICE 30.01.23

Who may we share your data with or receive it from?

Sometimes we need to share your information with others. We will only do this when it is necessary, or if we are required to do so by law. We do not plan to share it with anyone else or use it for anything else. When it is necessary, we may disclose footage to specific partners.

We may be asked to provide footage to assist the police with any criminal damage or their investigations.

However, there is no planned regular or scheduled sharing of CCTV footage with any external organisation. Should this situation change, this privacy notice will be updated and reissued, to keep you fully aware of how the Selkirk BIDS plans to use CCTV footage which you may be captured in.

CCTV footage will only be processed internally by nominated staff who are authorised to do so and any other parties where there is a legitimate and lawful reason for their involvement, such as in the event of an investigation.

How long is your data kept for?

This information is held in accordance with the Selkirk BIDS Retention Policy

What rights do you have over this use of your data?

- To be informed about how we use your data
- To access a copy of your data that we process
- To have us rectify or correct your data that we process
- To restrict our processing of your personal data
- To object to the use of your data
- To have your personal data erased
- To request that we transfer your information to you or another organisation
- To withdraw your consent (if it is the legal reason why we use your data)
- Some of these rights are subject to exceptions.

SELKIRK BIDS

CCTV PRIVACY NOTICE 30.01.23

Contact the Data Protection Officer:

If you have any concerns about how the Selkirk BIDS is using your data, you can contact the Selkirk BIDS Data Protection Officer by writing to:

DAVCANDERSON@AOL.COM

or write to us at:

48 High Street, Selkirk, Scottish Borders, TD7 4DD

If you are concerned about how your information is used by Selkirk BIDS please contact us using any of the above details. Alternatively, you have a right to complain to the Information Commissioner's Office

ICO Scotland contact details

The Information Commissioner's Office – Scotland

Queen Elizabeth House

Sibbald Walk

Edinburgh

EH8 8FT

Telephone: 0303 123 1115

Email: Scotland@ico.org.uk

Changes to our Privacy policy

Selkirk BIDS Privacy policy is subject to regular review, and we will update it when required.

This page is intentionally left blank