DATA PROTECTION IMPACT ASSESSMENT TEMPLATE

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process.

Are you looking to:

- Make an organisational change?
- Make a change in service?
- Gather new information on individuals?
- Make a change to an existing system?
- Introduce a new system?

A DPIA provides assurance that personal data is processed in accordance with the data protection principles. You should complete this form in as much detail as possible. The final outcomes should be integrated back into your project plan. Please read along aside the DPIA Template Guide.

If you would like some support, please contact the Information Management Team: dataprotection@scotborders.gov.uk

Department/Service/Team	Finance & Corporate Governance (Democratic Services)
Operational Information Asset Owner	Jenny Wilkinson
DPIA Author	Jenna Waldie

Version	Date	Author	Change
0.1	16 November 2021	Jenna Waldie	Initial draft based on meeting with Jon Laws, Shelagh Turnbull and Karen Farquhar
0.2	23 November 2021	Jenna Waldie	Changes to draft
0.3	24 November 2021	Jenna Waldie	Changes based on meeting with Shelagh Turnbull and Karen Farquhar
0.4	27 November 2021	Jenna Waldie	Changes based on information from Jon
0.5	6 December 2021	Jenna Waldie	Changes based on information from Alistair Langston and Marc Caulfield
1.0	7 December 2021	Jenna Waldie	Final draft circulated for discussion

Identifying the need for a DPIA

1.1 Please describe what are you trying to do, why and what the benefits are?

Background
At Scottish Borders Council we are committed to being as open and as transparent as possible. The Council is proposing to webcast meetings which would give members of the public the opportunity to watch live Council (meetings involving elected members) and committee meetings, as well as view an archive of previous meetings. The platform being explored to stream meetings is Live Events streamed through Teams. Anyone can access a published meeting on modern.gov.uk to watch a meeting back on demand.

In some instances, members of the public and guest speakers have the option to attend a meeting rather than only viewing the live meeting. For example, journalist. This risk will be addressed in this assessment.

Why are we doing this?
This is a new way of working as a result of the pandemic to continue democratic and Council process. This new way ensures the public are still involved. In response to continuing public health concerns around the pandemic, the Council initially agreed on 30 July 2020 that online meetings would be available to view via a livestream. From 10 August 2020, the public part of Council and all committee meetings have been livestreamed at the time of the meeting. However, no recording of the meeting is currently made and is not therefore available to view after the meeting has finished. In order to promote engagement with the community, officers have been looking at the means to be able to record meetings and make these available to the public after the event, in compliance with relevant legislation such as UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Human Rights Act 1998. Matters considered Official-Sensitive is not livestreamed and it is not intended that this part of a meeting will be recorded. Official-Sensitive is information regarding the business of the council or of an individual which is considered to be sensitive. This risk will be addressed in this assessment.

It is now proposed that the Council continues to livestream its online committee meetings when public business is being considered, but that these meetings are now recorded and made available to the public after the meeting through the link to the event livestream.

Meetings are generally held monthly however this differs for each meeting. Example of meetings include Full Council; Executive; Audit and Scrutiny Committee; Planning and Building Standards Committee; Licensing Committee; Area Partnership; and Common Good.

What are the benefits?
- Creates awareness and adds value;
- Attracts a wider audience;
- Easy and immediate online access using smart phones, iPads or other tablets, laptops or computers;
- No login required;
- No download time;
- Reduce number of information requests;
- Contact centres and libraries have public pcs available with internet access or access to Council websites, which members of the public can use to view meetings;
- Openness and transparency;
- For some meetings e.g. area partnerships it offers member of public to engage in live question and answer session;
- Opportunity for officers to revisit council meetings;
- Anyone can watch after the event (although a time limit applies to modern.gov.uk);

- Reduced carbon impact due to reduced need to travel;
- Observers can consume a part of the meeting without any disruption to the meeting; and
- Council owns the copyright in the webcast.

What are the disadvantages?

- Relies upon members of the public to have an internet connection and equipment;
- May need to download Microsoft Teams app if using Android or Apple;
- Internet connections, software and equipment aren't 100% reliable, they can all malfunction or fail;
- Will utilise any download allowance, bandwidth required for max 1080p resolution is 3Mbps;
- Members of the public may be unsure or unaware of how to watch the meeting due to lack of technical knowledge; and
- Understanding consequences of information being placed in public domain.

Future planning

It is further intended that when Council committees return to physical meeting rooms at Council Headquarters, either fully or in a blended manner, that any members of the public entering these rooms need to be aware that they may be filmed and those images and sound recordings may be used for webcasting. In this respect, signs will be displayed at the entrance to all Council meetings which are being webcast and recorded to tell attendees that this is happening. There will also be a notice on the agenda for the meeting. At the start of the meeting the Chair will announce whether the meeting is being livestreamed and recorded and the Chair will also have the discretion to terminate or suspend recording if in their opinion allowing recording to continue would prejudice the proceedings of the meeting. Unfortunately, the technology to be able to livestream and record physical/blended committee meetings will only be available at Council Headquarters for the foreseeable future. Therefore any meetings which take place elsewhere will not be livestreamed or recorded unless they take place wholly online.

The DPIA will be reviewed by the Information Asset Owner prior to making any change or if there is a change to any of the risk scoring to ensure compliance with all data protection principles and individuals rights.

1.2 Does the processing involve automated decision making, profiling or tracking?
This processing does not involve automated decision making, profiling or tracking.

Consultation

2.1 Please advise which stakeholders have been consulted while developing or reviewing the process?
Jenny Wilkinson Nuala McKinlay Shelagh Turnbull Karen Farquhar Jon Laws

Jenna Waldie
Marc Caulfield (CGI)
Alistair Langston

Elected Members will be consulted on 16 December after data protection impact assessment has been undertaken. Outcome of meeting will be reflected in this assessment.

Data Protection Principles

This section asks you to indicate how the processing will comply with each of the principles of data protection. Where you can, please provide evidence of what you have in place to achieve this, or clearly state what work is underway where you know there are gaps. You can provide links or attach any relevant documents.

PRINCIPLE 1: Fair, lawful and carried out in a transparent manner

- We obtain personal data from individuals in a manner that does not deceive or mislead as to the purposes of its collection
- We ensure that we provide a privacy notice that sets out who we are, why we need the information, what we will use it and how long we will keep it
- We ensure that personal data are processed with fairness and in compliance with all applicable legal provisions
- We ensure that the processing meets a lawful condition set out in Article 6 of the UK GDPR 2016
- We ensure that any processing of special category personal data meets a lawful condition set out in Article 9 of the UK GDPR 2016

3.1 Please state what is the lawful basis being relied on for this processing?

1. The individual has given their consent
2. In the performance of a contract
3. To meet a legal obligation
4. To protect the vital interests of individuals
5. In the performance of a task carried out in the public interest

Note: Consent of participants has been considered and this is not the most appropriate lawful basis. Relying on consent to record and publishing meetings is unmanageable. When relying on consent as a lawful basis to process personal data individuals have full control over how their information is used. The lawful basis will be kept under review and take into account any data protection concerns raised. Participants will be notified of processing prior to event and Chair will give option to turn camera off.

3.2 If relying on legal obligation or task in the public interest, please state the legislation that places an obligation, duty or empowers us to undertake the processing?

Section 50A of the Local Government (Scotland) Act 1973 governs admission to meetings of local authorities.

3.3 If the processing includes special category data, please state the condition under the UK GDPR?

1. The individual has given their explicit consent
2. Compliance with employment, social security and social protection law
3. Vital interests
4. Substantial public interest
5. Provision of health and social care
6. Occupational pensions
7. Not applicable

Note: Special category personal data will not be processed. However, it is recognised that religion for example, could be captured in a meeting.

3.4 if yes to the above and the processing involves criminal data or the processing is relying on 'substantial public interest' condition, please state the condition under the Data Protection Act 2018

1. Statutory and government purposes
2. Counselling
3. Equality of opportunity or treatment
4. Safeguarding of children and of individuals at risk
5. Preventing or detecting unlawful acts
6. Protecting the public against dishonesty
7. Safeguarding of economic well-being of individuals
8. Regulatory requirements relating to unlawful acts and dishonesty
9. Political parties
10. Preventing Fraud
11. Disclosure to elected representatives
12. Support for individuals with a particular disability or medical condition
13. Not applicable

3.5 What information is being provided to individuals through a privacy notice, how will it be distributed and in what format?

A privacy notice will need to be created and in place prior to recording and publishing meetings. Staff and members of the public can request a copy.

Engagement report functionality can be turned off by the meeting organiser. It is on by default, but can be ticked off. Information Asset Owner to determine if the engagement report is necessary.

☑ Attendee engagement report

A notice will be clearly placed on agendas which will be circulated prior to meeting. The Chair will announce whether the meeting is being livestreamed and recorded and by participating in the meeting, attendees understand this is part of the Council's public task. Participants are entitled to turn off video capability and raise any concerns with the Chair prior to the meeting taking place.

PRINCIPLE 2: Carried out for specified, explicit and legitimate purposes

- We record and document the purpose of the processing
- We ensure that the personal data is not used for another propose that is not compatible with the original purpose it was collected for
- We do not use personal data for another purpose without informing people in the first instance

4.1 Please state if you are changing the way personal data is being processed for an existing purpose or are you collecting data for a new purpose?

Scottish Borders Council is changing the way personal data is being processing for an existing purpose. The proposal is to publish live stream (audio, video and transcription) Council and committee meetings online. This is new processing as these meetings are not currently recorded. Meetings generally focus on Council matters. Meetings and recordings will not discuss matters that could result in the identification of a living individual. This risk will be addressed in this assessment.

4.2 Please state if the data may be used for another purpose in the future?

Scottish Borders Council will not use the data for another purpose in the future. This DPIA will be revisited if the council intends to use personal data for a new purpose to ensure it is compatible with the original purpose for processing.

PRINCIPLE 3: Is adequate, relevant and limited to what is necessary

- We only collect, use and store information that is relevant and necessary
- We ensure that personal data is only accessed by and/or shared with parties that need to fulfil the purpose
- We regularly review the data held, and delete anything not needed

5.1 Please state the categories of individuals whose personal data will be processed.

Employees
Elected Members
Participants such as members of the public e.g. journalist and guest speakers of other organisations e.g. Scottish Government, CoSLA, SOSE, Architects and NHS Borders

5.2 Please list the categories of personal data which will be processed and state why each is necessary and relevant.

Audio
Video
Transcription – Live event attendees can view live captions and subtitles in up to six languages in addition to the language being spoken. Event organisers can select the languages from a list of over 50.

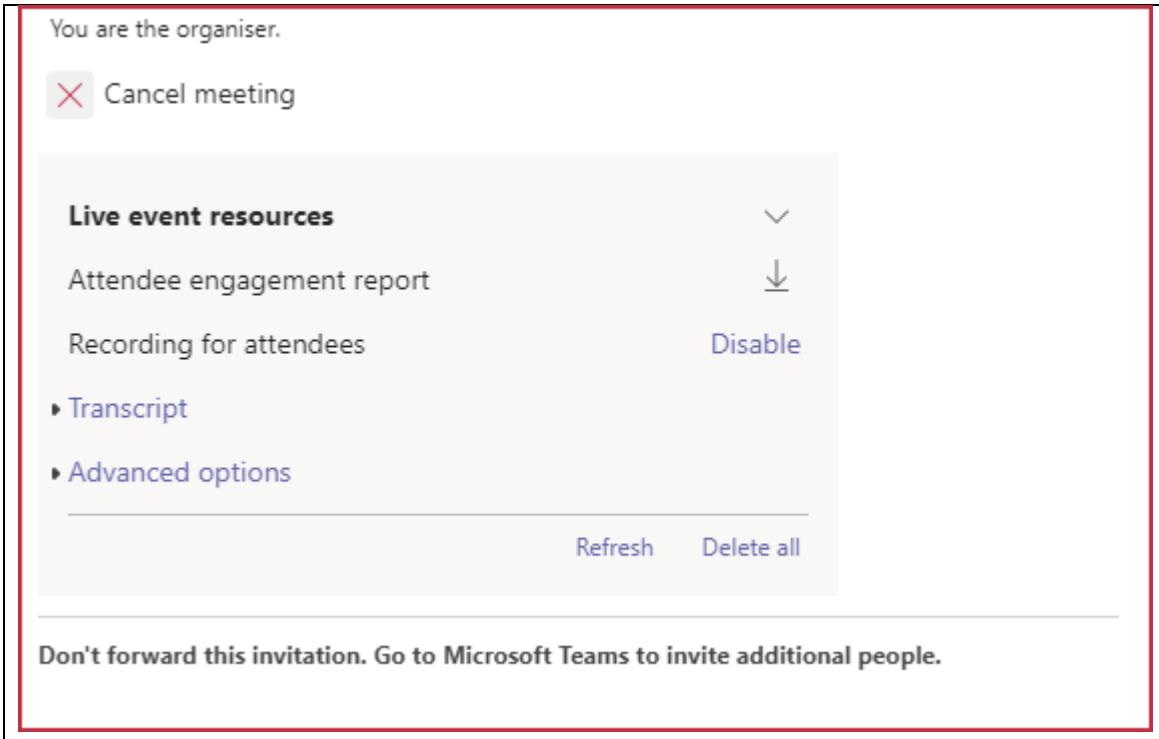
Personal image (incl. characteristics, age, ethnicity, gender, religion, disability) and voice of participant or person(s) in the field of view of a participant's camera or audible reach of their microphone.

People/objects in the field of view (blur or image backgrounds can reduce risks of capturing other persons or objects). Organiser, and/or recorder, of meeting to advise of switching on background when using a Teams app before any recording commences. If the participant is using a web browser version they should be mindful of people/objects/location that could be captured. All participants should make others (within their vicinity) that there will be recording. If not speaking in a meeting, the protocol should be that participants should mute their microphone.

No personal data and commercially sensitive data captured during live meeting. If the public business has ended, the meeting group moves into private and public meeting ends.

No IP address is captured.

Engagement report – name would show from member of public or guest if they have entered this information. For example, John Smith joined meeting on 16 November 2021 13:21 and left meeting at 14:30 and re-joined on. Users are given a code on the engagement report i.e. 7748466d-94ff-4f8e-9206-b02538032f08 is using an iPad. This information has been compared and the code differs for each meeting. This is not personal data. Email address also pulls through on the engagement report for participants e.g. JohnSmith@bbc.co.uk or JohnSmith@scotborders.gov.uk if they aren't connecting to the Teams Live Event as a guest or anonymous observer.



5.3 Please describe how the personal data will be collected.

Participants – meeting link (which may include external participants)
If participants are logged in to a 365 account, their email address and full name are recorded in the engagement report.

Viewers – live link (not joining physical meeting)

- Viewers use the live link that is published on the website for the meeting to access;
- Teams app opens on their chosen device;
- Viewers have the option to log in using their name and email address, if they have previously signed up to Teams or 365, or sign in as a guest where they can enter a name that they choose e.g. Mickey Mouse – verification is not required;
- If they log in with an established Teams or 365 account using name and email address this information is captured on the engagement report which can be downloaded by two officers (at present); and
- Audio and footage captured is not possible for viewers.

The engagement report can be downloaded through Teams by the organiser and or producer.

In some instances, staff ask who viewed their live event. Organiser and producer will be mindful that the engagement report may contain personal data e.g. email address and will consider data protection principles before sharing (verbally and electronically).

PRINCIPLE 4: Personal data must be accurate, and where necessary, kept up to date

- We ensure that there are appropriate processes in place to check the accuracy of the data collected, and record the source of that data.
- We have a process in place to identify for updating the data to properly fulfil the purpose(s), and update it as necessary.
- We keep a record of any mistakes and clearly identify it as a mistake.
- Record clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.
- We ensure that we can comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.
- We keep a note of any challenges to the accuracy of the personal data.

6.1 Please describe how the accuracy of personal data will monitored and maintained.

Audio and video is accurate 'as live' recording (which is subject to quality of participants camera/microphone/network quality).

Transcription is developing and improving speech to text recognition technology - transcription is not and will never be 100% accurate, there is always room for error. The quality of transcript varies depending on accents etc.

6.2 Please describe how any challenge to the relevance or accuracy of the personal data be managed.

If any member of staff receives any challenge or if any member of staff has a concerns this will be considered, discussed with Information Asset Owner, relevant Management and Information Management Team where required, and amended accordingly. Data protection concerns will be sent to dataprotection@scotborders.gov.uk and handled in line with the Information Commissioner's Office (ICO) process.

It is accepted that challenges may be received on meeting content. There is not an obligation to change records that the Council considers to be correct, but which the data subject (or their representative) disagrees. Although there is not a requirement to correct the record in these circumstances, it will normally be good practice for the relevant service to record the fact that they are disputed and why.

Any complaints, not relating to data protection (including data protection principles and individual rights), will be handled in line with Scottish Borders Council's complaints process.

PRINCIPLE 5: Personal data shall not be kept for longer than is necessary

- We ensure that personal data is not kept for longer than needed.
- We ensure that we are able to justify how long personal data will be kept for.
- We regularly review the data, and erase or anonymise it when no longer needed.
- We carefully consider any challenges to the retention of data to comply with Individuals' right to have the data deleted if it is no longer needed.

7.1 Please state the retention period that will be applied to the processing. We follow retention guidelines issued by the Scottish Council on Archives referred to as SCARRS.

Published recording automatically remains for 180 days. This is the default. This includes backed up data. If the service required it, there is the option to download and store elsewhere. Download option for members of the public will be marked as disabled.

It is unknown how long the engagement report stored in Team calendar on the live event entry remains for.

7.2 Please describe what the process will be for deleting all or parts of the data.

Teams is a cloud hosted solution therefore there is no guarantee information is permanently deleted. This risk will be addressed in this

Recordings are automatically deleted after 180 days.

However, if recordings stored elsewhere e.g. SharePoint this will trigger a different process and manual process. Recordings should not as practice be stored elsewhere.

PRINCIPLE 6: Personal data will be protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organisational measures

- We carry out an analysis of the risks presented by the processing, and use this to assess the appropriate level of security that is needed to be put in place.
- We take into account the state of the art and costs of implementation when deciding what measures to implement.
- We ensure that the Council's Information Security Policy is followed.
- Where necessary, we create additional policies and ensure that controls are in place to enforce them.
- We regularly review measures and, where necessary, improve them.
- We put in place basic technical controls such as those specified by established frameworks like Cyber Essentials.
- We put other technical measures in place if needed, depending on the circumstances and the type of personal data being processed.
- We use encryption and/or pseudonymisation where it is appropriate to do so.
- We understand the requirements of confidentiality, integrity and availability for the personal data being processed.
- We ensure that access to the personal data can be restored in the event of any incidents, such as by establishing an appropriate backup process.
- We conduct regular testing and reviews of the measures put in place 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 an approved code of conduct or certification mechanism.
- We ensure that any data processor used also implements appropriate technical and organisational measures.

8.1 Please state what organisational controls will be put in place to support the process and protect the data.
• Council staff required to complete Information Management (yearly), GDPR and Cyber Security training on SB Learn. • At the start of the meeting the Chair will announce whether the meeting is being livestreamed and recorded. • There are two layers of controls which can manage what is being broadcast. There are controls accessible by the Live Event producers but there are also controls within the core Team meeting. The organiser and the presenters in the Team meeting have a range of controls over all other participants. • The Chair or other officer can ask for an adjournment to terminate or suspend livestreaming and recording, either to receive advice from officers, or if in their opinion allowing livestreaming or recording to continue would prejudice the proceedings of the meeting.

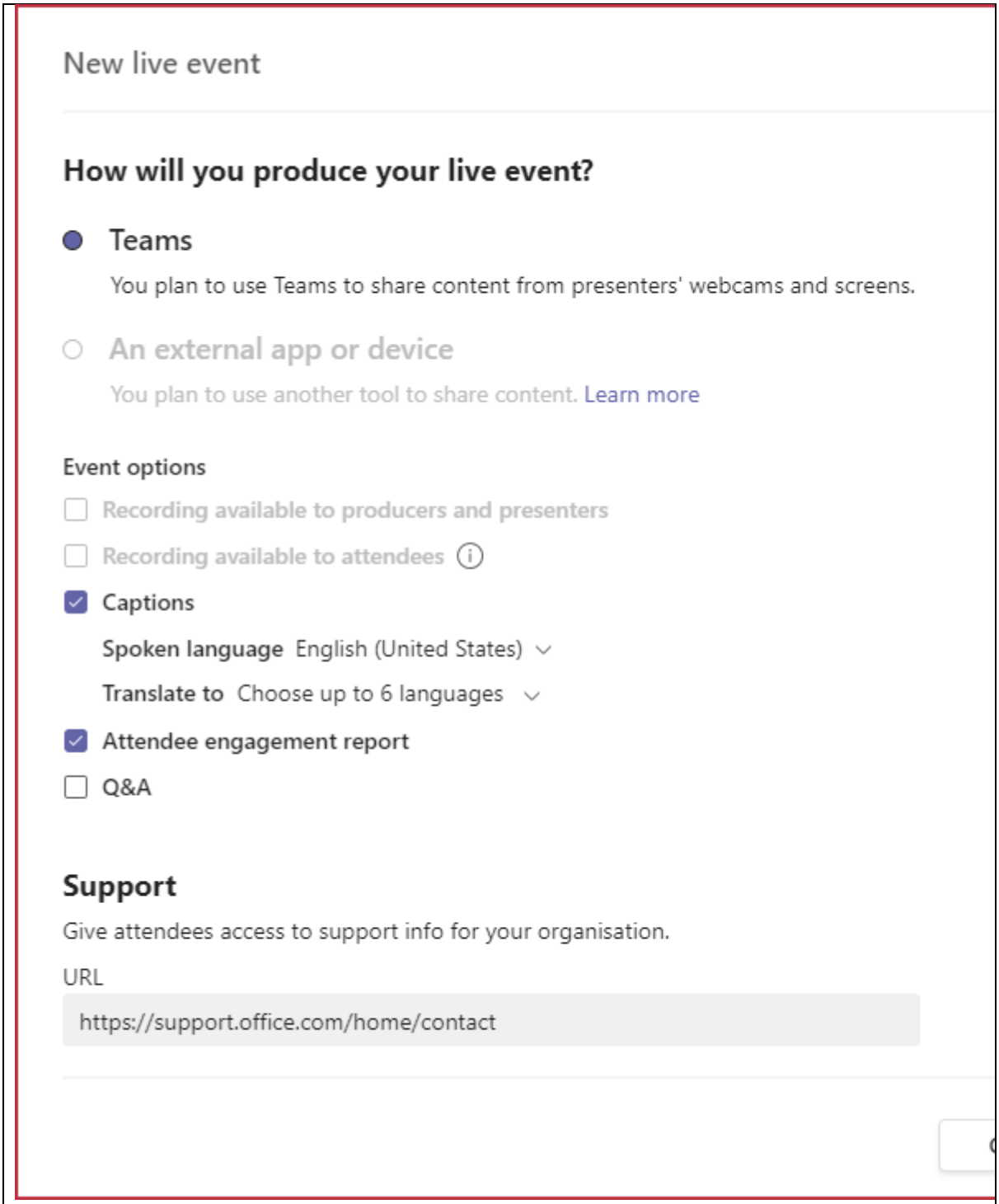
Circumstances that could lead to suspension or termination of webcasting include public disturbance or other suspension of the meeting or the potential infringement of the rights of any individual. If the meeting is to be 'ended' or 'adjourned' this should be instructed clearly and the Democratic Services Officer (DSO) will advise whoever is doing the live streaming. No-one else should give this instruction.

- Chairperson responsible for moving meeting from public to private and ensuring members of the public and guest speakers in attendance are not present if they do not need to be for their role. The meeting will ensure the live feed has ended before carrying on. Relevant member of staff will ensure everyone has left. If they have not, the organiser has the ability to remove participants.
- Agenda items, minutes and supporting documentation will not include Official-Sensitive information.
- Digital door – external participants wait in the lobby and can only be admitted by a DSO to the Teams meeting.
- Ability to mute and turn off participant's camera if required.
- Organiser has the ability to delete the live event, as well as disabling.
- Relevant officers participate in a Teams chat when a meeting is live to discuss concerns etc.
- Guidance and training is required for staff to ensure they understand what information can and cannot be livestreamed and ensure how they know how to present e.g. not share Outlook inadvertently. Information that is Official-Sensitive (personal data, commercially sensitive data etc.) should not be placed in the public domain. If this happens, and the recording cannot be edited, this cannot remain published.

8.2 Who will have access and how will this be managed?

Only the person (producers) in the live event area would have access to the engagement report - no-one else would be able to do anything here. At present, the number of staff with access is two, but this is subject to change.

When the meeting is published anyone will have access.



8.3 Please describe the technical measures that will be put in place to support the processing and protect the data (If CGI are involved, please provide a copy of their security assessment).
CGI has not undertaken an SIA for this processing.

Teams works in partnership with SharePoint, OneNote and Exchange. As far as SBC is concerned Data for each is stored as follows:

Service	Data at Rest
Exchange	European Union
SharePoint	United Kingdom
Skype for Business	European Union
Microsoft Teams	European Union

Teams enforces single sign-on through Active Directory, and encryption of data in transit and at rest. Files are stored in SharePoint and are backed by SharePoint encryption. Notes are stored in OneNote and are backed by OneNote encryption. The OneNote data is stored in the team SharePoint site.

8.4 Does the processing involve a data processor? If so, please confirm that legal has reviewed and agreed the contract. Please include what countries the data processor stores (including back-ups) personal data. If the data processors relies on sub-processors to process personal data, please include what countries they transfer personal data to and what measures they have in place to share.

****Important: if personal data is transferred outside of the United Kingdom, and in particular to the United States of America please contact the Information Management Team.****

Azure Media Services (AMS) from Microsoft, part of the 365 contract with Insight.

8.5 Will the information be shared with any other organisation? If so, please confirm that there is a data sharing agreement and include a copy/link with this DPIA.

The information will not be shared with any other organisation.

PRINCIPLE 7: Accountability

- We document our processing activities in writing and as part of these records we document:
    - information required for privacy notices;
    - records of consent;
    - controller-processor contracts;
    - the location of personal data;
    - Data Protection Impact Assessment reports; and
    - records of personal data breaches.

9.1 Please confirm that the Information Asset Register has been updated to include details of this this processing activity.
Who is the IAO?

Identify and assess risks

Identify measures to reduce risk

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** *Remote, possible or probable*	**Severity of harm** *Minimal significant or severe*	**Overall risk** *Low, medium or high*	**Options to reduce or eliminate risk** Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk	Effect on risk *Eliminated reduced accepted*	Residual risk *Low medium high*	Measure approved *Yes/no*
Risk that members of public and or guest speakers have left the meeting before moving onto private matters.	Remote	Minimal	Low	There is a formal move into private. The Chair has to do a motion to end live and the DSO checks relevant officers remain. Verbal confirmation is needed. Assurance check may be carried out by other officers – Skype chat	Reduced	Medium	
Risk that Official-Sensitive information is livestreamed and published. Official-Sensitive is information regarding the business of the council or of an individual which is considered to be sensitive.	Possible	Significant	Medium	There is guidance on the intranet under Information Management on what is considered Official-Sensitive. Specific guidance will also be created to reduce the risk of personal data or commercially sensitive information being is placed into the public domain.	Reduced	Medium	
Risk that staff with permission to remove content from the public domain is off work.	Possible	Minimal	Medium	Only the Live Event organiser can enable or disable the accessibility of a Live Event recording. As soon as it is known that a Live Event broadcast has exceeded an unsuitable for viewing threshold, the organiser can, under Manage Resources section of the Live Event in their Teams calendar, select disable	**Accepted?**		

				for the availability of the recording for attendees. This can be done during the broadcast of the Live event. The two Live Event producers are active during all Live Event broadcasts. The risk is only apparent if this determination of content being unsuitable for viewing is reached on a day after the event when the Live Event organiser is unavailable.			
Risk that too much personal data is processed e.g. people/objects in the field of view	Possible	Minimal	Low	Participants should blur or apply image backgrounds to reduce risks of capturing other persons or objects. Advising participants to have a bland background will reduce the risk of collecting information about their location and ensuring that is no personal data or special category personal data visible during the meeting. Organiser, and/or recorder, of meeting to advise of switching on background before any recording commences to ensure for example, children and or vulnerable people are not captured. All participants should make others (within their vicinity) aware that there will be recording. If not speaking in a meeting, the protocol should be that participants should mute their microphone.			

Risk that participants are not informed how their personal data will be processed via privacy notice.				Privacy notice is needed depending on outcome of engagement report.			
Potential duplicate recordings being stored				Council that it can't be saved anywhere else – council meetings? Can this functionality be removed/turned off?			
Risk that recordings are not permanently deleted in line with retention period and risk that recordings saved elsewhere are kept for longer than is necessary.				^^ Only the producers or meeting organiser can download an AV file of a recorded Live Event.			
Risk that the data controller/processor relationships are not sufficiently clear							
Inappropriate access for staff (staff not having correct access rights, not having access removed or granted in line with role changes)				2 members of staff at present			

Personal data is kept for longer than necessary				Teams is a cloud hosted solution. This means that the council is unable to guarantee information is permanently destroyed when deleted.			

Individual Rights

Data protection legislation provides individuals with certain rights over the processing of their personal data. The Information Management Team co-ordinates these requests, however it is important that processes are designed to support these rights.

Right to:	Control	Yes	No	N/A
Be informed	A privacy notice will contain the prescribed information and will be easily available.	**X**		
Access personal data	There will be procedures put in place to facilitate subject access requests in accordance with Council policy.	**X**		
Rectification	There will be a procedure put in place to ensure inaccurate data is rectified or enable a note to record any challenges.	**X**		
Erasure	There will be a procedure for fully considering and responding to these requests. Retention will be consistently applied to the data.			**X**
Restrict processing	There will be a procedure for dealing with requests to restrict data.	**X**		
Data portability	There will be a procedure put in place to transfer data upon request.			**X**
Object	There will be a procedure in place to ensure that objections to processing are properly considered and dealt with according to Council policy.	**X**		

3. Submission

Once completed, this DPIA should be sent to dataprotection@scotborders.gov.uk for the Information Management and Legal teams to review and provide feedback on behalf of the Data Protection Officer.

You will receive a report within two weeks, which will provide an assessment of the level of compliance with data protection based on the information provided in the DPIA. It may also contain recommendations on ways to improve that level of compliance, especially if what is proposed presents significant risks to the Council. If recommendations are made, you will need to provide confirmation that these have been addressed or actioned, or if not being undertaken, you will to provide the rationale for not auctioning. Once agreed with legal and IMT, the DPIA should then to be approved by the information Asset Owner (service operational lead).

It should be noted that this DPIA should be periodically reviewed and updated to reflect any changes or if any new risks are identified.

Approval

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by:		If accepting any residual high risk, the DPO must consult the ICO before going ahead.
IMT/Legal advice accepted or overruled by:		If overruled, you must explain your reasons.
Comments:		
This DPIA will kept under review by:		IMT should also review ongoing compliance with DPIA.