Scottish Borders Council

Income Management Policy

Contents

1. INTRODUCTION

The Income Management Policy supplements the Financial Regulations on Banking Arrangements, Income, Petty Cash, Cash Floats and Security and, therefore has the same standing as the Financial Regulations.

Managers must ensure that all staff within their service have read and understood the Income Management Policy and that they are complied with at all times. Furthermore, all staff involved in cash handling and banking should be made aware of the requirements of and have access to the Policy. Management and staff should be advised that disciplinary action may be taken against them if they fail to comply with the Policy.

The procedures represent the minimum standard that must operate throughout the Council. Managers may incorporate additional procedures only if they enhance the requirements of this Policy. Under no circumstances should the requirements of this Policy be reduced or omitted.

The Income Management Policy is intended to offer guidance to managers and staff on the minimum required procedures for the collection, control and banking of Council income. For the purpose of these Procedures income includes that received direct by cash, cheques, credit cards and debit cards and cash floats held on Council premises.

Daily processes may vary from service to service but this Policy is a corporate document that apply to all and must be adhered to at all times.

1.1 Objectives:

- All income received and held by the Council is completely and accurately accounted for and banked promptly
- All income is held securely
- Customers card data is not compromised

1.2 Why is this important?

- Income is a vulnerable and attractive asset. It can easily be misappropriated if not effectively controlled
- Effective controls over cash collection, retention and banking systems are necessary to ensure that all income due to or held by the Council is identified, collected, receipted and banked properly and promptly

1.3 What are the Key controls?

- All income due to or held by the Council is identified and charged correctly, in accordance with an approved charging policy
- All income is collected from the correct person, at the right time, using the correct procedures
- All income received by an employee on behalf of the Council is paid without delay to the correct reference/income code
- All income collected and deposited is regularly reconciled
- All income kept on Council premises is held securely

- All income is recorded in the Council's Income Management System (ICON)
- All income is monitored for budget purposes

1.4 Civica Icon – Income Management System

The Council uses the Civica Icon income management system for cash collection, income distribution, automated telephone payments, on-line payments and bank reconciliations.

Icon is the de-facto standard for all payment processing. All new IT systems with any income collection capabilities must utilise ICON unless there is written agreement from the Executive Director Finance & Regulatory on consideration of the business case to support an alternative approach.

All new systems not granted exemption must be capable of interfacing with ICON and its existing file formats. All new interfaces are by default the responsibility of the new system implementation team or project team and not the ERP Systems Support Team.

All new interfaces or extending the use of existing interfaces to new income streams must be agreed with the ERP Systems Support Team who will be responsible for testing any new interfaces, income streams or changes to existing interface and the Income and Reconciliation Team in advance of any development work commencing.

1.5 Roles and Responsibilities

Stakeholder	Key Role & Responsibilities
Customer	To make payment for goods or services received within the terms and conditions of the service provision.
Executive Director Finance & Regulatory (Section 95 Officer)	To be accountable for the effective management of income by Officers of the Council.
Corporate Management Team	To be accountable for the effective management of income by Officers of the Council.
Directors	Ensure Financial Regulations and the Scheme of Delegation in relation to the collection of income is adhered to. Ensure the parts of Corporate Policy & Strategy that apply to their directorate are correctly followed. Proactively support the achievement of corporate targets for debt collection. Ensure that Budget Managers are fully aware of their income management responsibilities.

Stakeholder	Key Role & Responsibilities
	Ensure that relevant income management systems and procedures are put in place. Ensure that employees involved in the income collection process are appropriately trained and the quality of training is kept under continuous review.
ERP Systems Support Team	Day to day administration and development of the Icon application. Setting up of all user accounts and user administrations on confirmation of training being undertaken. Setting up of all income stream system configurations Setting up and administration of importing and exporting of interface files. Ordering and coordination of chip and pin devices locations etc. Key point of contact with Civica. Key point of contact with CGI. Reconciliation of daily interfaces to and from Icon.
CGI	Responsible for infrastructure for which the application runs Ensure interfaces from and to feeder systems are enabled External whitelisted IP address is being used and registered with Civica Responsible for implementation of replacement of chip and pin devices Responsible for the locally hosted applications and transactional database
Income and Reconciliation Team	Ensures that the Council manages income effectively through the development and implementation of a corporate policy. Ensure that the right messages on the Council's approach to income management are conveyed to all stakeholders simply, clearly and effectively. Ensure that effective systems and procedures for financial administration are in place so that income collected and payments made are accurate, complete, timely and in accordance with legal and regulatory requirements. To discuss and promote action on consistent income management.

Stakeholder	Key Role & Responsibilities
	To promote and communicate income management and to involve all officers in the process. To scrutinise and provide assurance to directorate management on the processes and procedures. Ensures that proper accounting practice, reconciliation and control of the Income Management function.
Civica	Responsible for hosted application
Anyone that processes Income due to SBC	Raise the charge in a timely fashion either prior to or immediately following the provision of the goods or service. Ensure that the payment is processed efficiently immediately following receipt of the income. Escalate the recovery processes in a timely and controlled manner consistent with established procedures.
Anyone responsible for Income due to SBC	Provide simple documentation with clear information to help the Customer make payment easily and ensure that the payment is recognised by the Council's systems. Ensure that the procedures are clearly documented to enable those processing income to complete the transactions efficiently. Provide appropriate initial and refresh training to equip those involved in the processing of income to understand the systems and procedures under guidance from the ERP Systems Support Team. Maintain appropriate systems to record, process and store income data.

1.6 User Access and Training

Requests for a new users account must be requested by the individual's line manager.

Training modules on SBLearn must be completed before a new user account will be set up to ensure compliance and understanding of the Anti-Money Laundering Laws, Chip and Pin Security and Acceptable Use Policy for Chip and Pin 2013. A report from SBLearn will confirm when the modules have been completed. The Line Manager must also confirm that the Income Management Policy and Procedures have been read.

Only when appropriate training of new users has been carried out in conjunction with the issue and familiarisation of the Icon user manual and has been confirmed by the Line Manager will a valid user account be created and issued by the ERP Systems Support Team.

1.7 About this Policy

1.7.1 Who does this policy apply to?

These rules are applicable to all areas of the Council accepting, processing and raising any types of income, accepting cash or taking card payments

1.7.2 Who do I contact for further information?

For further information, please contact the following departments: -
Income and Reconciliation Team
Email complianceandcontrol@scotborders.gov.uk
Or
ERP Systems Support
Email businessworld@scotborders.gov.uk

1.7.3 Review of this policy document

This document is owned by the Income and Reconciliation Team and as such will be reviewed annually in January each year. Next review January 2022

2. INCOME MANAGEMENT SYSTEM

The Council's Income Management system, Icon, is supplied by Civica UK Ltd and was last upgraded in November 2019 to the latest available version.

The system is comprised of a Civica hosted, cloud customer facing application that is used for the taking and processing of all customer payments and a locally hosted, transactional database for the distribution of income to back office applications.

Hosted	Module	Function
1.	WebPayStaff	Enables the public to make either face to face or telephone assisted payments via cash, cheque, debit or credit card (inc chip and pin)
2.	WebPayStaff – Maintenance	Enables system administrators to set maintain the user base and system configuration parameters (inc payment options) within the system
3.	WebPayStaff – Reporting	Allows staff to run reports
4.	WebPayPublic	Allows customers to pay via the Internet
5.	ATP (Automated Telephone Payments)	Allows customers to make payments 24hrs a day over digital telephones
6.	PaylinkXML	Allows integrated payment with other applications (e.g. Jadu, Planning Portal etc.)

7.	ServicePay	Enable the easy setting up of miscellaneous templated payment streams
Local	Module	Function
1.	Workstation	Allows the journaling of bank suspense items
2.	Reporting	Allows users to report on all transactions
3.	Interface	Enables the importing of bank statements and transactional files and exporting of income received to back office applications
4.	Technical	Holds all the configuration of interface specifications and validation rules within the system
5.	Management	Enables the setup of back office users and system configuration
6.	eReturns	Enables banking returns to be submitted electronically
7.	Bank Reconciliation	Facilitates the automatic bank a/c reconciliations

2.1 System Administration

The Income and Reconciliation Team are responsible for all policy and procedures relating to the management and collection of income. The day to day administration and development of the system is carried out by the ERP Systems Support Team:

Function	Contact Details
New users and Password re-set	ERP Systems Support Team
Creation of new income streams System upgrades and development System Configuration	Businessworld@scotborders.gov.uk
Reports Payment Tracing Allocation of Income Reconciliation of Income	Income and Reconciliation Team at breturns@scotborders.gov.uk

2.2 Disclosures

Any members of staff with full administration access to Icon must have the appropriate PVG disclosure.

2.3 Sharing Passwords

Under no circumstances should members of staff share passwords. Such action would constitute a breach of the Password Policy.

2.4 Passwords

Hosted Modules
The minimum length of passwords is nine character long and must include alpha and numeric characters. Passwords will expire every 90 days and users cannot reuse any previously set passwords. User have 3 attempts to log into the application before they will be automatically locked out and will then need to seek assistance. If a user has not successfully logged into the system for 90 consecutive day's they user account will be automatically disabled.

Local Module
The length of the password must be between seven and eight characters long and alphanumeric. Password will expire every 365 days users cannot reuse any previously set passwords.

Should users have issues in logging into the system, they should contact the ERP Systems Support Team via emailing businessworld@scotborders.gov.uk

2.5 Leavers

Line Managers are responsible for informing the ERP Systems Support Team when users leave the Council or move from positions that require access to Icon.

3. RECEIPT OF INCOME

Each Officer is responsible for ensuring that all income due to their service is received and is completely and accurately accounted for.

All income received must be receipted immediately upon being received and must be recorded by the issue of an official Council receipt or cash register receipt. *(It should be noted that income received through the post may not be receipted immediately and should be recorded at the time of post opening pending transfer to staff for receipting.)*

3.1 Issuing manual official receipts

Manual receipts must only be issued where a cash register is not operated or where it is temporarily out of action, e.g. awaiting repair. Manual receipts must be dated, the payers name recorded and all required information completed. Only then should the receipt be signed by the member of staff collecting the income.

3.2 Receipt of Cheques

Where cheques are tendered by individuals at the time of payment or received in the post at HQ the following information must be written on the back of the cheque:-

The fund and reference number (eg CTax/NDR number, AR invoice number or FIS code) of where the income is to be posted to should be written on the back of the cheque along with the name and address of the person tendering the cheque where applicable.

- Personal cheques (staff and public) must not be exchanged for cash

- All cheques should be made payable to ”Scottish Borders Council“ and crossed “a/c payee only”. The location where the cheque was received should be identified clearly on the back

3.3 Post-dated cheques

3.3.1 All post-dated cheques received are to be returned to the payee unless the cheque is dated within a week of receipt. The cheques should be placed in a safe, to be actioned on the date of the cheque

3.3.2 Cheques returned to payees are sent with a cover letter explaining that we are unable to accept the cheque due to it being post-dated and ask them to amend the cheque and re-send it to SBC

3.4 Receipt of credit/debit cards

3.4.1 Card payments must be input straight into the Icon system. Card details must not be written down. If information is provided by the customer in writing, this information must be securely destroyed immediately after processing

3.4.2 Income from credit and debit cards will be controlled in much the same way as income received by cheque. Card validation will be carried out automatically by the system, but will need to be identified separately on banking records in order that the income can be traced by Finance when received through the banking system. This is because there is a delay in receiving income from these transactions

3.4.3 Copy Receipts must be kept secure and locked cupboard or safe. When receipts are being destroyed, they must be shredded and disposed of or placed in an appropriate confidential waste bin for disposal

3.5 Retention of Receipts

Copy Receipts should be retained in accordance with the Council’s document retention policy. At the moment this means they should be kept for the current year plus six.

4 CASH CONTROLS & SECURITY

Financial Regulations requires that each member of staff is responsible for ensuring that all income received is accurately accounted for and banked. In order to satisfy the requirements of these Regulations it will be necessary to establish and operate basic controls over cash, including cheques, and safes as follows.

4.1 Control of cash collected

Council insurance cover allows for up to £20,000 in a locked receptacle, e.g. till or cash box, and up to £50,000 in a locked safe or a strong room. Managers and the Internal Audit Service can place more restrictive limits to

encourage safer cash handling. Therefore, care should be taken to avoid amounts held at any time being in excess of the above limits or those imposed by Finance/Internal Audit. Regular banking should therefore take place to ensure cash does not build up.

Where cash and cheques are received the following controls must be applied:

- All cash and cheques must be held securely when on Council premises ideally in a safe or in lockable cash boxes where a safe is not provided. Insured limits must be adhered too

- Any floats must be held in a safe, or lockable cupboard/drawer or cash boxes for smaller amounts when not in immediate use

- Cash and cheques held before banking must be held in a safe or cash box pending the banking

- Access to safes will be limited to the delegated Cashier and or Manager

- Safe Keys must be held on the person of the authorised key holder at all times or alternatively stored in a key safe and must not be left unattended on the premises as this will invalidate insurance cover

- Till keys must be held on the person at all times and not left in the drawer

- Tills must not be shared and remain the responsibility of the cashier

4.2 Collection of CASH from parking ticket machines, toilets and school catering income.

4.2.1 Income from parking ticket machines and SBC toilets are now collected by a third party company and all monies are paid to an SBC bank account where it is reconciled and any discrepancies notified to relevant department and where necessary Internal Audit Department

4.2.2 The following procedure relate to machines that are controlled by the council, although School catering income is collected from the schools by a third party and adheres to the above (4.2.1) the following must be followed where schools use cash machines to allow contactless card payments at their own tills

4.2.3 All keys must be kept securely and only issued to and used by members of staff authorised to do so by the Cost Centre Manager

4.2.4 Cashing up – Machines

When it is required that machines are to be emptied the following procedure must be applied:-

- Machines must be emptied by two members of staff

- Those collecting the cash must jointly count, verify and record the income collected

A record of income collected from the machine must be maintained showing the following:

- Date of collection
- Cumulative meter readings, if available
- Income receivable according to the meter readings
- Actual cash taken
- Any overs or unders
- Signatures of the two members of staff undertaking the collection

4.2.5 Reconciling total income for collection by third party:

- Cash must be counted by two members of staff, verified and a record kept of the income that is being collected by courier
- All paperwork must be complete and initialled by two members of staff
- Ensure signature and receipt is received from courier on collection
- Income return emailed to banking return to enable reconciliation on receipt of funds into SBC bank account

4.3 Security of and Access to Safes

- Only authorised key holders will have access to the safes
- Whenever access to the safe will be required, a member of staff with authorised access will be on site
- Safe keys must be retained on the person of the authorised key holder at all times when on duty
- Safe keys must not be left on the premises overnight unless retained in a key safe
- Records of combination numbers must not be left on the premises at any time
- Where safe keys and/or combination numbers are given to a member of staff, the appropriate key register must be signed by the member of staff and Manager

- A safe may be open only when in immediate use and when a member of staff with authorised access is in the immediate vicinity

- Whenever an authorised key holder leaves the Council, changes employment or temporary cover ends, the Service Manager or designated person must ensure that the safe key is received and records updated

- Where an authorised combination holder leaves the Council, changes employment or temporary cover ends, the Service Manager or designated person must ensure that the combination of the safe is changed immediately

- Any loss of a safe key must be reported immediately to the Service Manager

4.4 Security of and Access to lockable cupboards, drawers or cash boxes.

Where safes are not operated the following must be applied:

All income must be stored in a lockable cupboard or drawer pending banking

- Where a cash box is used this must be stored in a lockable cupboard/drawer when not in use

- Access to the cupboard/drawer/cash box must be restricted

- Whenever access to the cupboard/drawer/cash box is required, a member of staff with authorised access must be on site

- Keys must be retained on the person of the authorised key holder at all times when on duty

- Keys must not remain on the premises overnight unless retained in a key safe

- The lockable cupboard/drawer/cash box must be open only when in immediate use; and when a member of staff with authorised access is in the immediate vicinity

- Whenever an authorised key holder leaves the Council, changes employment or temporary cover ends, the Service Manager or designated person must ensure that the safe key is received and records updated

- Any loss of a safe key must be reported immediately to the Service Manager

4.5 Security of and access to cash tills

- Members of staff authorised to use the cash till must be given appropriate training in cash handling and correct till procedures

- Cashiers must check the float with Supervisor on collection of till and agree balance

- Cashiers to ensure a maximum working float of £200.00 with surplus funds immediately transferred to a safe

- When the cash stored in the safe reaches £1000.00. The cashier must notify the Supervisor who will transfer the money to the main safe or arrange for it to be banked

- All income received must be processed immediately and placed in till

- Cashier keys, i.e. keys allocated to individual cashiers to gain access to the cash till (where used), must not be left in the cash drawer when not attended by the cashier

- Only the cashier logged on is to use the till during a shift

- All cash to be counted and totals confirmed in the presence of the customer before placing in till

- On receipt of over £1,000, monies must be double checked by another Customer Services Assistant in the presence of the customer

- Ensure customer has written the amount they wish to pay on a credit slip or shows invoice with amount due

- A receipt MUST be given for all cash deposits

- In the event of an incorrect amount being credited, the cashier must notify a Supervisor to carry out the reversal/partial refunds

- At end of shift, the cashier and Supervisor (or equivalent) must balance the till

- All totals to agree

- Any cash differences are to be investigated and if untraced-logged in the Cash Differences Register with both the cashier and Line Managers signature. Customer Services Co-ordinator and Income and Reconciliation Team complianceandcontrol@scotborders.gov.uk to be notified immediately of any differences

4.6 Routine checks

The senior manager must ensure that the following checks are performed, on at least a monthly basis, by a member of staff independent of the day to day

cash operation who must initial the records examined to confirm that the checks have been carried out.

- Review the key registers and Cash difference register to ensure daily records maintained with authorised signatories

- Balance petty cash float and agree totals

- Where irregularities are detected, the Senior Manager must be informed, Internal Audit notified and the matter investigated immediately

- Check that Chip and Pin devices have not been tampered with and that the cables and connectors are still in good working order

4.7 Voiding or cancelling transactions

It is recognised that on occasions staff will make errors when using cash till, e.g. press wrong key. This may involve an over or under ringing that will result in the need to cancel/void that transaction. The procedure in the Icon Customer Present user guide must be followed.

4.8 In the event of a fire/fire drill

Cashiers must log out of Icon, secure chip and pin devises as per Customer Service Policy and lock the cash till/drawer and take key with them.

5. CREDIT AND DEBIT CARDHOLDER DATA

5.1 Security Principles

Credit card processing includes paying on-line, by telephone and chip and pin and must follow specific security rules developed by the Payment Card Industry (PCI) Data Security Standards (DSS). Failure to follow the requirements can result in severe penalties, including fines and prohibition from further acceptance of the credit cards. Users should complete the Acceptable Use Policy for Chip and Pin 2013, Chip and Pin Security and PCI DSS Module in SBLearn to ensure compliance with security for credit card payments and information.

Card Details MUST NEVER be written down to be used later and always ask customers to repeat their details to you when checking you have the correct information required.

5.2 Credit Card Compliance

Departments which accept credit or debit card payments whether over the phone using Civicas's WebPay Staff or in public using a Chip & Pin device should ensure that all staff are aware of and comply with the relevant Payment Card Industry (PCI) Data Security Standards (DSS).

There should not be any stand-alone debit/credit card machines in the Council. Any enquiries about taking credit card payments or purchasing a credit card machine MUST BE directed to the Income and Reconciliation Team. All new card machines must be authorised by them.

5.3 New Chip and PIN machines

Face to face debit or credit card payments must be processed via a chip and pin machine linked to Icon. These devised are located in Contact Centres, Registrars and the Fleet office.

If there is a requirement to install new or replace existing chip and pin devices, the cost must be covered by each service. Enquires need to be emailed to the ERP Systems Support Team businessworld@scotborders.gov.uk who will request a quote direct from Civica.

Installation of devices are handled by CGI on the request of the ERP Systems Support Team.

5.4 Changes to an Existing Account

Changes to an existing merchant account must be approved by Income and Reconciliation Team or ERP Systems Support Team. Examples of changes are: purchasing, selling, discarding a terminal or purchasing software.

5.5 Credit Card Security Breach

If a potential credit card security breach is detected this must be reported immediately to Income and Reconciliation Team, ERP System Support Team, Internal Audit and Information Management Team.

Scottish Borders Council should be aware of:

- Suspicious behaviour – requesting refund to go to card not used in original transaction
- Transaction that might require further information eg name on invoice does not match card name
- Unusual incidents in audit logs
- User or anonymous report of problems
- Unauthorized security configuration changes
- Unusual traffic or activity
- Lapsed physical security eg holding onto card receipts beyond recommended timescales
- Sensitive information in the wrong place or hands
- User complaint which triggers an investigation
- Loss or theft of a computer or a chip and pin device

5.6 Resolving credit / debit card queries

On occasions it may be necessary to resolve a payment query, resulting from system or network issues.

Staff are **NOT PERMITTED** to transmit, process or store credit card information on Council computer systems or the Internet. The name, address, contact number and details of the query should be obtained from the customer and then if department is unable to resolve the issue it may be necessary to contact the Income and Reconciliation Team or ERP Systems Support Team where further guidance will be given.

5.7 Segregation of duties

Establish appropriate segregation of duties. Staff handling credit card processing are not permitted to authorise refunds back to a card. These are handled via Income and Reconciliation Team and ERP Systems Support Team when required.

5.8 Credit Card Data Retention

Credit card transaction date for both card holder present and card holder not present are held within Icon for 2 years.

6. CASH BALANCING AND BANKING

- All income collected must be balanced on a daily basis by comparing the total of the cash, cheques and credit/debit cards to the receipt totals

- All income received by the Council must be banked intact. Under NO circumstances must retentions or deductions be made to the takings to be banked

- Any shortages in income identified during the cashing up process must not be made up from other sources

- All overs and shortages must be recorded and any significant or persistent discrepancies reported immediately to the Manager and the Income and Reconciliation Team by email to complianceandcontrol@scotborders.gov.uk

- Banking should be made on a regular basis with the minimum being twice per week and always on the last day of the month. Timescale may vary for each area – Customer Contact Centre

- Insured limits must be considered in the retention of income pending banking

- All income must be supported by sufficient documentation to ensure that it can be adequately identified and accounted for. This will include the

recording of seal numbers on the paying in slip where sealed security bags are used

- Care must be taken to ensure that paying in slips are completed clearly in order that income can be identified and allocated correctly

- Banking should be made at the nearest Bank, Post Office or Mobile Banking Unit to the office. Where set banking days have been established try to vary the time of day if possible that staff take funds. If a banking day falls on an official bank holidays then banking may be done on the first appropriate working day following the official holiday

6.1 Daily Cash Balancing

- Daily cash balancing must be completed by two members of staff

- The income must be jointly counted, verified and recorded

- Cash books such as Income Returns must be completed showing totals for cash and cheques against the relevant income codes. Credit/debit card transactions must also be recorded a per Income Return/Cash Book

- The reference numbers on the bank paying-in slips must be cross referenced with the income banking sheet submitted to banking returns

- Any irregularities must be reported to the manager immediately

6.2 Cash Banking

When transporting cash/cheques to a bank or post office it is extremely important that all safety measures are followed. The aim is to reduce the risk of exposing personnel to attack and/or injury, whilst carrying money.

The following measures must be adhered to at all times, however they are only the minimum standards and where possible additional precautions should also be taken.

- Up to £2,500 - One person carrying, plus a mobile phone/two way radio

- £2,500-£5,000 – Two persons carrying, plus a mobile phone/two way radio

- £5,000+ - the sum must be split and banked at different intervals

- Regularly vary the time of day where-ever possible that banking is undertaken. As above banking can be made at a bank, post office or mobile banking unit

- If attacked, or attempts made to steal the bag carrying the money – Under no circumstances should personnel attempt any act of bravery

- Always hand over the money to any person attempting to steal the money

- Do not attempt to either fight off or fight back against any attacker as this only increases the risk of serious injury

- Hand over the money and, when able to do so, raise the alarm by calling firstly the Police and then the Council

- Your personal safety is of paramount importance to the authority. The money stolen can be replaced. You cannot!

7. REFUNDS

7.1 Refunds to cards

Refunds to cards are usually made on the same day from ICON where a mistake has been made by the cashier. If it is required to be refunded at a later stage directly to a card, the refund authorisation paperwork must be completed, authorised and sent to Income and Reconciliation Team via breturns@scotborders.gov.uk mailbox or where payment has been made through the MyScotBorders account, notification from Jadu will be received to confirm refund which will be processed through ICON.

Once the transaction has reached the target system e.g. Council Tax the refund should be initiated from that system.

Below is a table indicating the correct method of refund

Payment made by bank transfer	Refund to originating bank utilising Bacs.
If payment made by cheque	Proof required of account that cheque came from. Refund to that account will be made by BACS using source system.
If payment made via the web	Refund to original card via Webstaff.
If payment made by credit card	Refund to original card via Webstaff
If payment made in cash	Refund by BACS to bank account

7.2 Refund Cheques

The Council would prefer to make electronic payments which are both more efficient and cost effective. Every effort should be made to gather information so that payments can be made electronically.

8. REPORTING OF IRREGULARITIES

Any member of staff who thinks that there may have been a theft or other case of misappropriation of the Council's income must inform their line

manager immediately. The line manager must then inform their Service Director and Audit and Risk Department.

Where it is suspected that their line manager may be involved then the Service Director and Internal Audit Service should be informed.

Any member of staff who has any queries with regards to the Banking and Cash Handling Procedures must ask their line manager for assistance. If the query is not answered then advice can be sought from the Income and Reconciliation Team, ERP Systems Support Team or from Internal Audit Service. Please use the following emails for any queries:

complianceandcontrol@scotborders.gov.uk
breturns@scotborders.gov.uk
businessworld@scotborders.gov.uk