Scottish Borders Council

Income Management Policy

Contents

Appendices – Work Procedures

1. INTRODUCTION

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

Managers must ensure that all officers within their service have read and understood the Procedures 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 Procedures.

The procedures represent the minimum standard that must operate throughout the Council. They are designed to protect the best interests of the Council and to ensure that staff who are involved in income collection are supported and protected in carrying out their duties.

The Procedures contained within the policy are intended to set out the standards required of managers and staff involved in 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 any cash floats held on Council premises.

Daily processes may vary from service to service but the Procedures are 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 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 Chief Financial Officer 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 and not the ICON Administration Team.

All new interfaces or extending the use of existing interfaces to new income streams must be agreed by the Corporate Finance Manager in advance of any development work commencing.

Icon issues receipts for all face to face transactions and only providing receipts for postal remittances where a stamped addressed envelope is provided. Internet payments will be given the option for the customer to print off their own receipt.

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	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 & s95 officer.	• 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. • Ensure that Budget Managers are fully aware of their income management 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.
Corporate Finance Manager	• Responsible for managing all income to the Council • Business owner of the Income Management System • Ensures that the Council manages income effectively through the development and implementation of a corporate policy and strategy. • Ensure the income channels are easily and widely accessible. • 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.
Accounting Services Manager	• Manages the team responsible for maintaining and developing the Income Management System and controls. • To discuss and promote action on consistent income management. • To promote and communicate income management and to involve all officers in the process. • To coordinate training activities to ensure that a core competency on Income Management is maintained within the directorate. • 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.

Stakeholder	Key Role & Responsibilities
Anyone that processes Income due to SBC	• Raise an invoice using the AR system ICON 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. • Maintain appropriate systems to record, process and store income data.

1.6 Training

The Council has in the past allowed training to be passed down from one user to another. This has diluted the skill base in the use of ICON and the awareness of money laundering and Payment Card Industry Data Storage Standards.

Once the training has been completed staff will be required to sign a document to provide evidence that the training has been completed and that they are aware of this policy document and other related policies and procedures.

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 cash or taking card payments.

1.7.2 Who do I contact for further information?

For further information, please contact the Corporate Finance Manager Tel 01835 825019 or the Accountancy Services Manager. Tel: 01835 824000 x 5338

1.7.3 Review of this policy document

This document is owned by the Corporate Finance Manager and as such will be reviewed annually in January each year. Next review January 2013.

1.8 Awareness of Council Policies

Before a member of staff is set up on ICON they will be asked to read the following related policies:

No.	Name of Policy	Owner
1.	Corporate Debt Recovery Policy	Finance
2.	Corporate Charging Policy (Sept 2012)	Finance
3.	Computer Security and Standards Policy	BTS
4.	Information Security Policy	BTS
5.	Anti Money Laundering Policy	Finance
6.	Corporate Anti Fraud Policy	Audit & Risk
7.	Use of E-mail and the Internet	BTS
8.	Password Policy	BTS
9.	Customer Care Policy	Customer Services

Staff will also be made aware of the following legislation:

No.	Name of Legislation
1.	Data Protection Act 1998
2.	Terrorism Act 2000
3.	Anti-Terrorism Act 2001
4.	Proceeds of Crime Act 2002
5.	Money Laundering Regulations 2007
6.	Bribery Act 2010

2. INCOME MANAGEMENT SYSTEM

Icon is the name of the Council's Income management system and it is supplied by Civica UK Ltd. The software that the Council currently operates is version 8.1 and this was upgraded in 2009. The latest release is version 11.0.

The software is made up of various modules.

No.	Module	Function
1.	Workstation	Cash Receipting for face to face transactions
2.	Webstaff	For taking card payments over the telephone
3.	Web Public	Allows the public to make card payments on the web
4.	ATP	Allows the public to make payments 24hrs a day over the telephone
5.	Paylink	Allows integrated payments with other applications(eg CRM)
6.	Reporting	Allows staff to run reports
7.	Maintenance	Allows administrators to set parameters within the system
8.	Bank Reconciliation	Facilitates automatic reconciliations with the bank.
9.	E-Returns	Allows banking returns to be submitted electronically. This is currently in development.

2.1 System Administration

The Corporate Finance Manager is the business owner of the Icon system and is responsible for all policy and procedures. The day to day administration of the system is carried out by the Shared Services Team:

Function	Telephone Number	Email Address
Passwords, Reports	01835 824000 x 5944	Shared Services - Reports, Training and Reconciliations ssrtr@scotborders.gov.uk
Development Work	01835 824000 x 5575	Shared Services Development ssd@scotborders.gov.uk
Payment Tracing, Suspense accounts,	01835 824000 x	Shared Services Operations sso@scotborders.gov.uk

2.2 New Users

If a new user is required to be set up the form in appendix 1 should be completed and signed by the head of service and forwarded to the ssrtr@scotborders.gov.uk mail box. The shared services team will then contact the new user to arrange a suitable time for training which will take place at HQ. The form can also be found on the intranet.

2.3 Disclosures

Any member of staff with **full administration access** to the Icon system must have had an enhanced disclosure check.

2.4 Sharing Passwords

Under no circumstances should members of staff share passwords. Such action would constitute a breach of your terms and condition of employment.

2.5 Passwords

Passwords should be a minimum of nine characters long and contain a mixture of alpha and numeric characters. Once Icon has been upgraded this will be enforced centrally.

Should you forget your password you should contact the Shared Services Team on 01835 824000 x5944. Because so many of the Council's staff are located in remote offices it is difficult to validate the identity of individual members of staff so you may be asked for a council telephone number where a member of the shared services team can call you back.

2.6 Password Reviews

Passwords should be reviewed every 30 days. Once Icon has been upgraded this will be enforced centrally.

2.7 Unauthorised Access Attempts

The shared services team monitor daily any unauthorised access attempts. Any breaches of policy will be referred to the Corporate Finance Manager for resolution.

2.8 Plug and Play Media Ports

For those users of ICON who utilise Workstation or Webstaff the USB and CD/DVD ports will be disabled in order to meet PCI compliance standards.

2.9 Leavers

Line Managers are responsible for informing the Shared Services Team when members of staff leave the Council so that their username can be disabled.

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,

The fund and reference number of where the credit should be posted should be written on the back of the cheque along with the name and address of the person tendering the cheque.

- 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 – See appendix 11

3.4 Receipt of credit / debit cards

3.4.1 Card payments must be input straight into the Icon system or relevant card terminal. 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, i.e. card validation, 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 Where income is received by the use of credit/debit cards, it must be determined that the card is current before the payment is accepted and a receipt issued.

3.4.4 Copy Receipts must be kept in a locked safe. When receipts are being destroyed, they must be shredded and put into confidential waste bags which must be sealed.

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 officer 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

Sections 4.1 – 4.5 of the policy have been redacted form the public document as they relate to security procedures and the safety of staff.

4.2 Collection of CASH from vending machines, telephones and parking ticket machines.

4.3 Security of and Access to Safes

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

4.5 Security and access to cash tills

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, Audit notified and the matter investigated immediately.

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. Where these occur please inform a supervisor who will carry out the refund/reversal.

4.8 In the event of a fire / fire drill

Cashiers must lock the cash till/drawer and take key with them.

5. CARDHOLDER DATA

5.1 Security Principles

Credit card processing (e.g. on-line, by phone, card swiping) should follow specific security rules developed by the Payment Card Industry (PCI) Data Security Standards. Failure to follow the requirements can result in severe penalties, including fines and prohibition from further acceptance of the credit cards.

5.2 Credit Card Compliance Certification

Departments which accept credit card data must be compliant with Payment Card Industry (PCI) / Data Security Standards and undergo a verification process through SBC's credit card authorisation server utilising the Council's Income Management System – ICON.

There should not be any stand alone debit/credit card machines in the Council after 1st July 2012. Any enquiries about taking credit card payments or purchasing a credit card machine MUST BE directed to the Corporate Services Manager or the Accounting Services Manager. All new card machines must be authorised them.

5.3 New Chip and PIN machines.

To take credit cards securely face to face a chip and pin machine is required. These will be deployed in contact centres, libraries and museums across the council. Any additional machines will have to be purchased by the service requiring it once approval has been sought from the Accounting Services Manager.

If at any time you have a question or concern about accepting credit cards, please contact the Shared Services Team.

5.4 Changes to an Existing Account

Changes to an existing merchant account must be approved by The Accounting Services Manager. Examples of changes are: purchasing, selling, or discarding a terminal; purchasing software.

5.5 Incident Response Plan

If a potential credit card security breach is detected, **Shared Services Staff** are to be alerted. Scottish Borders Council should be aware of:

- Suspicious behaviour (i.e. name on invoice does not match credit card name)
- Unusual incidents in audit logs
- User or anonymous report of problems
- Unauthorized security configuration changes
- Unusual traffic or activity
- Lapsed physical security
- Sensitive information in the wrong place or hands
- User complaint which triggers an investigation
- Loss or theft of a computer or backup media

5.6 Resolving credit / debit card queries

On occasions it may be necessary to resolve a payment query, resulting from system or network issues. In these cases it will be necessary to contact the shared services team.

In general staff are NOT PERMITTED to transmit, process or store credit card information on Council computer systems or the Internet. When cardholders visit Council Websites be directed to the ereceipts page

5.7 Prevent unauthorised access to cardholder data

Establish procedures to prevent access to cardholder data in physical or electronic form including but not limited to the following: hard copy or media containing credit card information must be stored in a locked draw or office; staff should ensure visitors sign logs and ensure escorts are used to restrict access to documents, servers, computers and storage media.

5.8 Transmitting credit card information by email or fax

Full or partial credit card numbers and three and four digit validation codes (usually on the back of credit cards) may not be faxed or emailed.

5.9 Storing electronically the CVV, CVV2 validation code, or PIN

Do not store the CVV, CVV2 validation code from the credit card or the PIN, personal identification number.

5.10 Segregation of duties

Establish appropriate segregation of duties between staff handling credit card processing, the processing of refunds, and the reconciliation function.

5.11 Imprint Machines

Do not use imprint machines to process credit card payments as they display the full 16 digit credit card number on the customer copy.

5.12 Credit Card Data Retention

There are two types of transactional data.

- With Card holder data
- Without card holder data

Transactional Card holder data

Card holder data is retained so that automated refunds and reversals can be performed. Once the window for refunds and reversals is over then there is no requirement to hold these details.

The retention of card data on servers is managed by the Shared Services Team with support from BTS and Civica.

Cleansed Transactional data

Transactional data without card holder details is required to be held for accounting purposes and for disputes and Charge back requests.

For the purpose of Charge back disputes there is a requirement from cards schemes to have transaction data retained. This is to be able to provide the scheme with the relevant evidence to support the chargeback request.

The data retention period specified by the schemes is as follows.

Card Scheme	Retention Period
Visa / Debit / Electron	12 Months
UK Maestro /Solo	24 Months
International Maestro	24 Months
MasterCard	18 Months
JCB	18 Months

To facilitate this requirement the Council must keep all Merchant copy receipts for Card holder present transactions for the time frame defined and be able to produce a customer receipt for any Card Holder not present transaction.

In short this means that the Council must retain copy receipts for card payments for 24 months but there is not a need to keep the full card number as the customer receipt only displays the last four digits.

For all transactions older than 24 months the card details are not required so they can either be truncated or removed completely.

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.

- Bankings should be made on a regular basis with the minimum being twice per week. Timescale may vary for each area – Customer

Contact Centre, Crematorium, Car Park Ticket Machines (dependant on the amount of income that gets received and the safe limit that has been imposed).

- 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 is slips are completed clearly in order that income can be identified and allocated correctly.

- Where set banking days have been established these must be adhered to, with the exception of official bank holidays where banking may be done on the first appropriate working day following the official holiday.

6.1 Daily Cash Balancing

- Daily cash balancing should 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 as per the Income Return/Cash Book.

- The reference numbers on the bank paying-in slips must be cross referenced with the income return number.

- Any irregularities must be reported to the manager immediately.

6.2 Cash Banking

This section of the income management policy has been redacted from the public document as it relates to security procedures and the safety of staff.

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, this should be referred to the Shared Services Team.

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 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 if possible

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

The manager to whom the matter has been reported must inform the Head of Service, the Chief Financial Officer, the Corporate Finance Manager and the Head of Audit & Risk.

Any member of staff who has any query 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 Internal Audit Service.

Appendix 1

Civica Icon – New User Form

Name of new user: **Dept**
Team

Job Title:

Name of Line Manager: **Location / Building**

Has the new user been subject to a disclosure as part of their employment?

A Disclosure is a document containing impartial and confidential criminal history information held by the police and government departments which can be used by employers to make safer recruitment decisions.

	Module Name	Description	Yes / No
Modules Required	Workstation:	Face to Face Transactions	
	Webstaff:	Telephone Transactions	
	Reporting:	To view transactions:	
	E-Returns:	To input banking returns electronically	
	Refunds:	Supervisor level to initiate refunds for card payments only.	
	Bank Rec	HQ staff only	

Access to Civica Icon will only be given once the member of staff has been given the appropriate training. Following receipt of the signed form, from the head of service, the Shared Services team will arrange for the staff member to attend HQ as soon as possible.

Head of Service Name

Signature:

Date:

A copy of this form will be kept in the following directory for reference:

Appendix 2

Civica Icon – Leavers Form

Name of new user:	**Dept** **Team**
Job Title:	
Name of Line Manager:	**Location / Building**
Date left employment	

It is the responsibility of the employee's line manager to ensure that the Shared Services Team is notified when a member of staff leaves the employment of the Council. By not informing the Shared Services Team as soon as possible you are increasing the risk of potential fraud.

Head of Service Name	Signature:
	Date:

Appendix 3

Cashier Receipting Procedure

- Select Workstation from icons
  Login - code (3 numbers)
  Password
  F12 to enter

- Select from top buttons whether you are processing a single, multiple or batch payment
- Single payment enter
  - Reference number (council tax/rates/journal/accounts receivable corresponding reference number)
  - Fund (05-council tax/06 accounts receivable/07 rates/99 journal)
  - Amount – check invoice corresponds with cheque/cash (no decimal point)
  - MOP – (01 cash/02 over the counter cheque/03 posted cheque/04 postal orders) – there is a list attached of all other MOP and Fund codes
  - Enter through the amounts and accept the transaction
  - Receipt options
    - Default receipts are only used if temporary receipts are unavailable and you require an official receipt.
    - Multiple receipts are used for Council Tax cards (select the next appropriate week to receipt against)
    - Temporary receipts are for official receipts or select default if temporary unavailable.
    - N for no receipt.

    Accounts receivable payments require receipts if handed in at counter but not if it comes through post. Place receipt in printer
  - Print cheque option is available for over the counter cheque payments if and when requested.
  - Finally place cheque in printer (upside down) to print transaction on the back.

- Multiple payment enter
  - Reference (council tax/rates/journal/accounts receivable)
  - Fund (05-council tax/06 accounts receivable/07 rates/99 journal)
  - Amount – check invoice corresponds with cheque/cash (no decimal point)
  - At this point the screen will return to the reference point to continue to input the multiple entries. Once completed the total on the right should match the payment.
  - MOP – (01 cash/02 over the counter cheque/03 posted cheque/04 postal orders) – there is a list attached of all other MOP and Fund codes
  - Enter through the amounts
  - Finally hit end to finalise the multiple payment
  - Accept the transaction

- Receipt options
  - Default receipts are only used if temporary receipts are unavailable and you require an official receipt.
  - Multiple receipts are used for Council Tax cards (select the next appropriate week to receipt against)
  - Temporary receipts are for official receipts or select default if temporary unavailable.
  - N for no receipt.

  Accounts receivable payments require receipts if handed in at counter but not if it comes through post. Place receipt in printer
- Print cheque option is available for over the counter cheque payments if requested.
- Place cheque in printer to print transaction on the back.

- Journals
  - Journals are received throughout the day and all information should be supplied
  - Enter the provided reference code
  - Fund code is always 99
  - Provide a informative narrative from the journal or pink slip
  - Enter amount
  - Enter VAT code which will always be provided
  - MOP
    - Accounts journals - From entries are 81 (out) and To entries are 80 or your normal cheque/cash options

- Planning cheques
  - Multiple
  - Funds 18 & 99

- Finalising banking in afternoon

  - Select from the F1 cash up button
  - Enter in the relevant banking amounts in the corresponding boxes
  - Check to make sure that the total entered and the expected amount agree.
  - Select the full cash up button and ok through all the printing options
  - Insert yellow paper to print

  - Select cash up from top menu
  - Select banking
  - Select the Add
  - Select your sign in (keeping the Dr/Cr cards separate from the cheque and cash)
  - Dr/Cr cards
    Select Main Account
    Ref-HQ70
  - Cheques and cash
    Select main account
    Ref- 00000800

Include bag reference, select OK and exit using Alt F12

Appendix 4

Webstaff Procedure

Webstaff - Electronic payment collection
Sequence of actions for taking a WEBSTAFF payment.

1. Go to Intranet home page – click on “Applications” – click on “Webstaff”

2. Enter your 3 digit USER ID and your PASSWORD and click on “SIGN ON”, then click on the option “New Payment – Cardholder Not Present”

3. You will now be in the “Webstaff – New Payments” page

4. From the drop down box pick the FUND you require

5. Enter the Reference (Council Tax (10 digit) NDR (9 digit) Accounts Receivable (8 digit) Registrars (10 digit) etc.)

6. Enter the AMOUNT (Pounds & pence separated by a point e.g. 10.00)

7. Enter a NARRATIVE (This should be meaningful – Often a name or address)

8. If you are happy with the details entered and the system has validated them click ADD or if you want to re-enter click CLEAR. If you “ADD” the details will be displayed on a new line and the fields already entered will clear, allowing you to enter a second (or more) account(s) for payment if required. Continue to click ADD after entering the details for each account

9. Enter the CARD TYPE as advised by the customer from the drop down list

10. Enter the CARD NUMBER as advised by the customer. After entering the number read it back to the customer for confirmation. DO NOT WRITE IT DOWN

11. Enter the ISSUE NUMBER as advised by the customer (Not all cards have one, some have a 1 or 2 digit number)

12. Enter the ISSUE DATE (use the drop down list)

13. Enter the EXPIRY DATE (use the drop down list)

14. Do not enter the CUSTOMER NAME & ADDRESS as this information is not captured

15. If you are happy with the entries click ACCEPT and wait for the screen to display confirmation (If you do NOT want to process the payment for any reason at this stage, then click CANCEL). Click ACCEPT again when the confirmation is received. A receipt is displayed and the customer can be advised of the receipt number if they are happy that this is a sufficient receipt. If required the receipt can be emailed to the customer by entering their email

address and clicking SEND or the screen page can be printed off and posted to the customer.

16. MAIN MENU takes you back to 3. above (New Payment – Cardholder Not Present) ready for the next transaction

Appendix 5

CREDIT/DEBIT CARD PAYMENTS PROCEDURE

Payment for any Council service may be accepted by Cr/Dr card. The procedure is quite simple and on-screen instructions are provided as you go along.

Process:
Enter the payment details as normal in either the Single or Multiple transaction screens, using MOP 70.

At the point when you are normally asked if you want to accept the transaction, the 'ENTER DETAILS' screen will be displayed.

Hold the card with the black strip facing you and to the bottom of the card then swipe it through the reader on the keyboard from right to left.

You should then see a pop-up box asking 'Do you want to accept this transaction?' – press enter or click yes to accept.

(If the reader fails, click the 'Manual Input' box, key the details from the front of the card and press enter. The details required are different for each type of card. Complete all the boxes you can – the system should know what is/is not required e.g. no issue no. for a Switch card.)

You will then be shown the 'CHECK DETAILS' screen – do this and press enter or click OK if you are satisfied they are correct. (So far the details have always agreed with the card. If they do not then 'Escape' from the transaction in the usual way and try again.)

The system will then hang for a few seconds showing 'AWAITING ACQUIRER RESPONSE' while the payment is authorised by the payer's bank. The screen should then show 'Authorisation Successful' – press enter or click OK. (If the payment is not authorised, follow the on-screen guidance e.g. refer the cardholder to his own bank.)

Press enter or click OK to print the Receipt (confirmation) for signature by the customer. This consists of two sheets of paper one white, one yellow. Print the white copy first, followed by the yellow. Align the pages with the white copy on top and pass to the customer for signing. As the paper is carbonised, the signature will appear on both copies, but the white copy will show the full card number whilst the yellow will have all but the last four digits blanked out.

Check the signature against the card and press enter or click OK if correct.

Proceed with any receipt(s) as normal.

Return the card, the yellow copy of the signed confirmation and any receipt to the customer. Retain the white confirmation for our records.

File the white copies of the signed confirmations in date order in a secure place.

Appendix 6

Cash handling and system Procedures

The three paragraphs below are instructions which apply to cashing up procedures, over and under balances when cashing up and the voiding of transactions within the cash system.

These instructions are being issued following points being raised by our External Auditors during their annual inspection. In particular instruction (3) under "Cashing up…" procedures is not being followed in all offices and must be from now on as must the overs and unders procedures.

All staff must read, understand and adhere to these instructions.

Team Leaders/Line Managers must ensure staff receive instructions and training as required and that these procedures are being followed at all times. With regard to signing off the Cashing up reports a non Supervisor may sign off when no
Supervisor is available however Team Leaders should ensure this does not occur regularly i.e. more than once or twice per week per
office.

Appendix 7

Cashing up & end of day procedures

1. At end of day, count cash and deduct opening float and total non-cash items individually and in total (cheques, card payment vouchers & postal orders)

2. In “cash-up screen” agree cash and non-cash items. In the event of a mismatch, recheck figures. Follow procedure below for over & unders if mismatch is not resolved. Complete the “full cash-up “ screen option.

3. Print transaction etc. reports as prompted and have them authorised by a Supervisor whenever available. A non Supervisor may authorise then in the occasional circumstances when a Supervisor is not available.

4. Fill in the bank pay-in slip but do not seal the bag at this stage.

5. Carry out the “system banking” using “banking” option on the toolbar ensuring that cash, cheque and postal orders totals agrees with pay-in slip.

6. Ensure bank bag number is written on pay-in slip. Seal bank bag.

Appendix 8

Dealing with overs & unders Procedures

Each Local Officer Supervisor is responsible for identifying over and unders. They should then take the following action:

- For amounts below £20 they should record the occurrence and investigate how it has occurred. The relevant Team Leader should be notified.
- If there are regular overs or unders occurring or consistent occurrences by the same cashier the Team Leader should investigate. They should record their findings and if necessary inform the Revenues Manager and Internal Audit.
- For amounts between £20 and £100 the relevant Team Leader & Internal Audit should be notified immediately. The Team Leader should carry out the investigation and record details. If necessary the Revenues Manager should be informed.
- For amounts over £100 the Revenues Manager and Internal Audit should be notified immediately.
- Banking should not be delayed because of an under or over.
- The ledger print and the radius report on overs & unders should be reviewed monthly by a Revenues Manager.
- In any case if you are sure that it is due to a theft or a break in the office you should notify the Police immediately.

Appendix 9

Voiding Of Transactions Procedure

Members of staff should no longer void any transaction within the cash system without the prior consent of a Supervisor. In future the requirement for a transaction to made void should be raised with a Supervisor prior to it being made void and the routine below followed.

The supervisor will confirm whether they agree the transaction should be made void.
They will complete the attached Transaction Void form with all details and observe the transaction being made void.
The Supervisor and cashier will sign and date the form confirming the transaction has been made void.
Paper copies of the signed form will be retained by the Supervisor at each Contact Centre who will ensure when required they are accessible to Internal and External Audit.

This routine will continue from the date of this email until such time as an acceptable electronic system is in place or a secure system based authorisation process is in place.

Appendix 10

Responsibilities of
Credit Card Handlers and Processors

(Supervisors – please copy this section and have all credit card handlers and processors return a signed to the Shared Services Team to be kept on file.)

As a credit card handler or processor I agree to abide by the provisions in this document. If I need further clarification I will refer to "The Scottish Borders Income Management Policy"

I **will NOT** do the following:
1) Acquire or disclose any cardholder's credit card information without the cardholder's consent including but not limited to the full or partial sixteen (16) digit credit card number, three (3) or four (4) digit validation code (usually on the back of credit cards), or PINs (personal identification numbers).
2) Transmit cardholder's credit card information by e-mail or fax.
3) Electronically store on a Council computer file or server any credit card information.
4) Use an imprint machine to process credit card payments. (An imprint machine is a non-electronic portable device that slides over a customer's credit card and displays the full 16 digit credit card number on the customer copy.)
5) Share a computer password if I have access to a computer with credit card information.

I **will DO** the following:
1) At time of employment, agree to complete a background check within the limits of local law.
2) Change a vendor-supplied or default password if I have access to a computer with credit card information.
3) Password-protect my computer if I have access to credit card information on a computer.
4) Escort and supervise all visitors including SBC personnel in areas where cardholder information is maintained or processed.
5) Store all physical documents or storage media containing credit card information in a locked drawer, locked file cabinet, or locked office.
6) Report immediately a credit card security incident to my supervisor, the Shared Services Team and the Accounting Services Manager if I know or suspect credit card information has been exposed, stolen, or misused.

Supervisor in writing
The Shared Services Team by email @ sso@scotborders.gov.uk

(This report must not disclose by fax or e-mail any credit card numbers, three or four digit validation codes, or PIN numbers. It must include a department name and contact number.)

_____ _____
Signature Date

_____

Print Name

Appendix 11

Xxxx Xxxxxx
Chief Financial Officer

Xxxx Xxxxxx
Corporate Finance Manager

Date: …….
Ref: ……

XXXXXXXXXXXXX
Address 1
Address 2
Address 3
Post Code

Dear XXXXXXXXXXXXXXXXXXXX

Re: Return Of Post Dated Cheques

I refer to the recent cheque that you have send to Scottish Borders Council for £XXXXXX.99 This cheque is **post dated** and therefore the Council is unable to accept it as a legitimate payment. It has been returned to you with this letter.

Please make arrangements to make this payment again using one of the options below:

By Debit or Credit Card :–

- online - http://ereceipts.scotborders.gov.uk (available 24/7)
- Automated Telephone Line - 01835 826500 (available 24/7)
- Assisted Telephone payment Service 0300 100 1800 (office hours)
- In person at one of the Council's 11 contact centres (office hours)

By Cheque made out to Scottish Borders Council posted to the address at the bottom of this letter.

Yours sincerely

Corporate Finance Manager