FAREHAM
BOROUGH COUNCIL

Report to
Portchester Crematorium Joint Committee

Date: **15 June 2015**

Report of: **Treasurer to the Joint Committee**

Subject: **FINANCIAL REGULATION 12 – INCOME AND BANKING**

RECOMMENDATION

(a) That the revised Financial Regulation 12 be approved.

REGULATION 12: INCOME COLLECTION AND BANKING

Income is collected by the Crematorium in relation to:

- **Cremation Fees**
- **Ashes**
- **Use of Organ**
- **Book of Remembrance**
- **Memorial Card**
- **Donation to Garden Improvement Fund**

All income collection processes must be handled with care to avoid loss or theft.

12.1 OVERVIEW

12.1.1 **Fees and Charges:** Officers must keep under review the level of fees and charges and any other levies made for services under their control.

Together with the Treasurer to the Joint Committee they shall report to the Joint Committee at least annually on the need to vary existing charges and introduce new charges.

12.1.2 **Credit Agreements:** Any agreement which allows the extension of credit payment facilities must be agreed in advance with the Treasurer to the Joint Committee.

12.1.3 **VAT on Income:** Officers must ensure that all employees collecting income establish the appropriate tax treatment on each transaction they deal with.

12.1.4 **Responsibility for Income Collection:** All arrangements for the collection of income are subject to the approval of the Treasurer to the Joint Committee. Officers are responsible for ensuring that all income due is brought into account.

12.1.5 **Timing of Collection:** Income due to the Crematorium shall be recovered by collection at the point of service or in advance, wherever possible.

12.1.6 **Collection Methods:** The income collection methods employed should ensure the efficient and prompt collection of income due.

12.1.7 **Controlled Stationery:** All receipting devices, debtor accounts, forms and other documents of a like nature shall be ordered and controlled by the Manager and Registrar.

12.2 INCOME COLLECTION

12.2.1 **Counterfeit Notes**: Any bank notes received in person should be checked to ensure they are genuine before they are accepted.

12.2.2 **Records of Income Collection:** Appropriate records must be maintained of all payments received through the post or in person; these should be updated at the time of collection. This will usually be by means of issuing till receipts or completing official receipts; however, in some cases the use of registers or logs may be more appropriate.

12.2.3 All payments received via electronic transfer, direct debit, BACS, cheque or some other non-cash method do not require a formal receipt unless requested by the payer.

12.2.4 **Personal Cheques:** Personal cheques or other such payments must not be cashed out of monies held on behalf of the Crematorium.

12.2.5 **Security:** Appropriate arrangements must be made for all income collected to safeguard against loss or theft.

12.2.6 **Direct to Bank Collections:** Income, which is collected directly to the Crematorium bank account, must be processed promptly into the Crematorium's financial accounting systems and in accordance with credit card procedures.

12.3 TRANSFER AND BANKING

12.3.1 **Timing of Banking:** Cash and cheque receipts by the Crematorium shall be passed to the Crematorium's bank within a maximum period of 5 working days.

12.3.2 **Total Income Banked:** No deduction shall be made from income collected, unless written approval has been given by the Treasurer to the Joint Committee.

12.3.3 **Banking of Cheques:** Every Officer of the Crematorium who pays money into the banking account of the Crematorium, shall ensure that the following particulars of each cheque paid in are recorded:

a) the amount of the cheque;
b) a reference (such as the number of the receipt given or the name of the debtor), which will connect the cheque with the debt or debts in discharge or partial discharge of which it is received.

Exemption from this rule is allowed if it can be demonstrated that this information is held securely on a Crematorium system, which provides a clear audit trail to the cheque transactions, included in a banking transaction.

12.3.4 **Reconciliation of Ledger Transactions:** Cash and cheque transfers prepared for banking must be regularly reconciled to income posted to the Crematorium's accounting system. These reconciliations should be reviewed by the Manager and Registrar.

12.3.5 **Reconciliation of Bank Statements:** All income prepared for banking must be regularly reconciled weekly to the Crematorium's bank account statements.

12.4 RECOVERY AND WRITE-OFFS

12.4.1 **Recovery Procedures:** Officers must establish and initiate appropriate recovery procedures, including legal action where necessary, for debts that are not paid promptly.

12.4.2 **Write-Off Authorisation:** Debts due to the Crematorium may only be written off:-

a) by the Treasurer to the Joint Committee where the amount for any one debtor is less than £5,000.

b) in all other cases by the Joint Committee.

12.4.3 **Case Details:** Authorisation for write-off will only be given on receipt of debt particulars (debtor, amount and nature of debt) plus a summary of recovery action taken.

12.4.4 **Records:** A record must be kept of all write-offs authorised and actioned which is totalled at the end of each financial year.

12.5 CARD PAYMENTS

12.5.1 **Information Security Policy:** Portchester Crematorium handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect the cardholder data, cardholder privacy, and to ensure compliance with various regulations, along with guarding the future of the organisation.

12.5.2 Portchester Crematorium commits to respecting the privacy of all its customers and to protecting any customer data from outside parties. To this end Officers are committed to maintaining a secure environment in which to process cardholder information. Employees handling sensitive cardholder data should ensure:

- Handle Company and cardholder information in a manner that fits with their sensitivity and classification;
- Protect sensitive cardholder information;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval;

- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;

12.5.3 Information security incidents must be reported, without delay, to the Manager and Registrar.

12.5.4 **Protect Stored Data :** All sensitive cardholder data stored and handled by Portchester Crematorium and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by Portchester Crematorium for business reasons must be discarded in a secure and irrecoverable manner.

12.5.5 If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed.

12.5.6 PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chats, ICQ messenger etc.

12.5.7 It is strictly prohibited to store:

- The contents of the payment card magnetic stripe (track data) on any media whatsoever.
- The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
- The PIN or the encrypted PIN Block under any circumstance.

12.5.8 **Information Classification:** Data and media containing data must always be labelled to indicate sensitivity level.

- Confidential data might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to Portchester Crematorium if disclosed or modified. Confidential data includes cardholder data.
- Internal Use data might include information that the data owner feels should be protected to prevent unauthorised disclosure.
- Public data is information that may be freely disseminated.

12.5.9 **Access to the Sensitive Cardholder Data** : All Access to sensitive cardholder should be controlled and authorised. Any job functions that require access to cardholder data should be clearly defined.

- Any display of the card holder should be restricted at a minimum to the first 6 and the last 4 digits of the cardholder data.
- Access to sensitive cardholder information such as PAN’s, personal information and business data is restricted to employees that have a legitimate need to view such information.

- No other employees should have access to this confidential data unless they have a genuine business need.

12.5.10 **Physical Security** : Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. “Employee” refers to full-time and part-time employees, temporary employees and personnel, and consultants who are “resident” on site. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to physically enter the premises for a short duration, usually not more than one day.
- A list of devices that accept payment card data should be maintained.
-

Asset/Device Name (Make / Model)	Description incl Serial Number / Identifier	Owner / Approved User(s)	Location

- The list should include make, model and location of the device.
- The list should have the serial number or a unique identifier of the device
- The list should be updated when devices are added, removed or relocated
- POS devices surfaces are periodically inspected to detect tampering or substitution.
- Personnel using the devices should be trained and aware of handling the POS devices.
- Personnel using the devices should verify the identity of any third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Personnel using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel. Strict control is maintained over the external or internal distribution of any media containing card holder data and has to be approved by management.

- Strict control is maintained over the storage and accessibility of media.
- All computer that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

12.5.11 **Protect Data In Transit:** All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Card holder data (PAN, track data, etc.) must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send cardholder data via email or by any other mode then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, SSL, TLS, IPSEC, etc.).
- The transportation of media containing sensitive cardholder data to Fareham Borough Council Civic Offices must be undertaken by the Manager and Registrar or Deputy Manager and Registrar, with the media delivered to the Treasurer to the Crematorium or Deputy Treasurer to the Crematorium.

12.5.12 **Disposal Of Stored Data** : All data must be securely disposed of when no longer required by Portchester Crematorium, regardless of the media or application type on which it is stored.

- An automatic process must exist to permanently delete on-line data, when no longer required.
- All hard copies of cardholder data must be manually destroyed when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic cardholder data has been crosscut shredded in a timely manner.
- All cardholder data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media. If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.

12.5.13 Incident Response notifications to various card schemes

1. In the event of a suspected security breach, alert the Manager and Registrar or Deputy Manager and Registrar immediately.
2. The Manager and Registrar or Deputy Manager and Registrar will carry out an initial investigation of the suspected security breach.
3. Upon confirmation that a security breach has occurred, the Manager and Registrar or Deputy Manager and Registrar will begin informing all relevant parties that may be affected by the compromise.

VISA Steps

If the data security compromise involves credit card account numbers, implement the following procedure:

- Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
- Alert all affected parties and authorities such as the Merchant Bank (your Bank), Visa Fraud Control, and the law enforcement.
- Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.
- Complete Visa Incident Report Template
- For more Information visit: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_ compromised.html

MasterCard Steps:

I. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.
II. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to compromised_account_team@mastercard.com.
III. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
IV. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
V. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
VI. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
VII. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have

been compromised and group all known accounts under the respective parent member IDs.

2. Distribute the account number data to its respective issuers.

Employees of the company will be expected to report to the security officer for any security related issues. The role of the security officer is to effectively communicate all security policies and procedures to employees within the company and contractors. In addition to this, the security officer will oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in both this document and at the training sessions and finally, oversee the implantation of the incident response plan in the event of a sensitive data compromise.

Discover Card Steps

I. Within 24 hours of an account compromise event, notify Discover Fraud Prevention at (800) 347-3102
II. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
III. Prepare a list of all known compromised account numbers
IV. Obtain additional specific requirements from Discover Card

American Express Steps

I. Within 24 hours of an account compromise event, notify American Express Merchant Services at (800) 528-5200 in the U.S.
II. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
III. Prepare a list of all known compromised account numbers
IV. Obtain additional specific requirements from American Express