Stonehaven Tolbooth Association
(Tolbooth Museum)

A Scottish Charitable Incorporated Organisation
SC043279

CONFIDENTIALITY & DATA PROTECTION POLICY

All personal information will be regarded in the first instance as confidential. Both the user and the donor of the information need to be able to trust the organisation to respect their confidence.

Any disclosure of confidential information to any other person may only be undertaken with the expressed permission of the donor for the purpose of assisting or protecting the individual, when information shall be shared with the appropriate authority.

Any breaches of confidentiality whether legitimate, inadvertent or deliberate will be treated with the utmost seriousness. Action will be taken to educate/discipline those involved. All staff are bound by this confidentiality policy. Deliberate breach of confidentiality would constitute gross misconduct.

The Board of Trustees has overall responsibility for ensuring that the Confidentiality Policy of Stonehaven Tolbooth Association (STA) is regularly reviewed and that all staff, volunteers and clients are aware of their responsibilities regarding the use of confidential information in the organisation.

What Information is Confidential?

All personal information should be regarded in the first instance as confidential. Both the user and the donor of the information need to trust the organisation to respect their confidence. All personal information is confidential, - whether **Written**, **Spoken**, **Observed** or **Electronic.** This includes but is not limited to:

Staff information name, address, telephone, email address, information included in job application forms, references, annual reviews, medical details, financial details.

Volunteer information (including Board of Trustees) name, address telephone, email address, information obtained in application forms, references, medical details, support & supervision reports.

Who has Responsibility?

Board of Trustees has overall responsibility.

Staff and volunteers have a duty to maintain confidentiality in their work.

All staff have responsibility for maintaining physical security of records and information.

Who has Access?

The Data Protection Act 1998 requires that individuals have access to the information held about them.

All clients and volunteers have the right to know about the content of any records held about them that have been originated by STA.

In all other circumstances confidential information should be accessed on a need to know basis only.

Staff Information

- Board of Trustees - members will require access to staff details during recruitment process or during any grievance or disciplinary procedure.

Data Handling & Security

STA will comply with the eight principals of good data handling as described in the Data Protection Act and make sure personal information is: .

1. used fairly and lawfully
2. used for limited, specifically stated purposes
3. used in a way that is adequate, relevant and not excessive
4. accurate
5. kept for no longer than is absolutely necessary
6. handled according to people's data protection rights
7. kept safe and secure
8. not transferred outside the UK without adequate protection

Accurate and Relevant

Ensuring that all information held is relevant and accurate is vital. Make clear what are facts and what are views and comments. STA recommend holding only factual information required to carry out the work of the organisation.

Security of information is paramount. Extra care is required where KDP shares office space with other organisations.

Paper

- Lockable filing cabinets are essential for storing information held in paper files.
- Ensure that keys are held securely.
- Do not leave open filing cabinets unattended.
- A clear desk policy can ensure that files are only taken out of the filing cabinet for a short time while in use.
- Take care when leaving information in filing trays, on desks and in the photocopier.
- Personal information should not be left on notice boards, notepads or open diaries.
- Take care when passing confidential information.

Electronic and other media

- Take care that confidential conversations are not overheard.
- Do not leave confidential information on answer machines.
- Computer held data should be password protected.
- Screen savers should be password protected.
- When writing down passwords ensure they are stored securely. Take care that passwords are not overheard.
- Do not leave computers switched on and unattended.
- Ensure that computer disks and other storage devices are held in a lockable storage container.
- A secure email system is essential – ensure minimal confidential information is passed in this way.

Out and About

- Take care not to identify clients or volunteers when producing publicity leaflets, press releases or at other public events.

Retention & Destruction

- Keep personal information only for as long as is required.
- Client and volunteer records should be kept for 5 years after support has ended.
- Financial records kept for 7 years.
- Employment and staff records for 7 years after termination of employment.
- Regular reviews should be carried out of information held to identify and dispose of all outdated and unnecessary information.
- All confidential paper information should be shredded before being discarded.

Informing Staff, Volunteers & Clients

- Confidentiality is part of the induction and training process for staff and volunteers.
- All members of the organisation are to be made aware of the Confidentiality and Data Protection Policy.

Breaches of Confidentiality

Any breaches of confidentiality whether legitimate, inadvertent or deliberate will be treated with the utmost seriousness. Action will be taken to educate/discipline those involved.

Secure Handling, Use, Storage and Retention of Disclosure Information

For the purpose of this policy PVG Scheme records, PVG Scheme Record Updates, Standard and Enhanced Disclosures will be referred to as Disclosure Records.

Introduction

The Code of Practice ("the Code") is published by Scottish Ministers under section 122 of Part V of The Police Act 1997 ("the 1997 Act"). The Code sets out obligations for registered bodies, counter signatories and other recipients of disclosure information

issued by the 1997 Act and the Protection of Vulnerable Groups (Scotland) Act 2007 ("the 2007 Act").

General Principles

1. STA complies with the Code and the 1997 and 2007 Acts regarding the handling, holding, storage and retention of disclosure information provided by Disclosure Scotland. We comply with the Data Protection Act 1998 ("the 1998 Act"). This policy is available to anyone who wishes to see it on request.

2. Disclosure records will be requested only when necessary and relevant to a particular post and the information provided on a disclosure record will be used only for recruitment purposes.

Usage

3. We will use disclosure information only for the purpose for which it was requested and provided. Disclosure information will not be used or disclosed in a manner incompatible with that purpose. We will not share disclosure information with a third party unless the subject has given their written consent and has been made aware of the purpose of the sharing.

Handling

4. STA recognises that, under section 124[1] of the 1997 Act and sections 66 and 67 of the 2007 Act, it is a criminal offence to disclose disclosure information to any unauthorised person. Disclosure information is only shared with those authorised to see it in the course of their duties. STA will not disclose information provided under subsection 113(B)(5)[2] of the 1997 Act, namely information which is not included in the certificate, to the subject.

Access and Storage

5. We do not keep disclosure information on an individual's personnel file. It is kept securely in lockable, non-portable storage containers. Access to storage units is strictly controlled and is limited to authorised named individuals, who are entitled to see such information in the course of their duties.

Retention

6. To comply with the 1998 Act, we do not keep disclosure information for longer than necessary. For the 1997 Act, this will be the date the relevant decision has been taken, allowing for the resolution of any disputes or complaints. For the 2007 Act, this will be the date an individual ceases to do regulated work for us. We will not retain any paper or electronic image of the disclosure information. We will, however, record the date of issue, the individual's name, the disclosure type and the purpose for which it was requested, the unique reference number of the disclosure

[1] The Serious Organised Crime and Police Act 2005 ("the 2005 Act") schedule 14, paragraph 12 amended section 124

[2] Subsection 163(2) of the 2005 Act inserted subsection 133B into 1997 Act. Subsection 113B(5) of the 2005 Act replaces subsection 115(8) of the 1997 Act

and details of our decision. The same conditions relating to secure storage and access apply irrespective of the period of retention.

Disposal

7. We will ensure that disclosure information is immediately destroyed in a secure manner, i.e. by shredding, pulping or burning, STA will ensure that disclosure information which is awaiting destruction will not be kept in any insecure receptacle (e.g. a waste bin or unlocked desk/cabinet).