the National Trust for Scotland

a place for everyone

Data Protection Policy

CONTENTS

Data Protection Policy and Guidelines

1. PURPOSE

This policy is intended to define the policy and principles adopted by The National Trust for Scotland's (The Trust) to govern the processing of personal data as specified in the Data Protection Act 1998. Management and staff must have an awareness of the obligations imposed by the Act and, depending on the nature of the information being stored or processed, take appropriate steps to ensure that the Trust complies with the legislation.

Through its day to day operations the Trust is required to collect and hold certain types of information about a variety of business contacts. These include customers, suppliers, current, past and prospective employees, volunteers, members, donors, potential donors and others with whom it communicates. In addition, it may occasionally be required by law to collect and use certain types of information of this kind to comply with the requirements of government departments for example, business data. The Data Protection Act includes safeguards to ensure personal information is dealt with properly regardless of how it is collected, recorded and used, whether on paper, in a computer or recorded on other material

2. LEGISLATIVE FRAMEWORK

The current Data Protection Act was introduced in 1998. "The Act" is intended to protect the rights of individuals whose personal data is stored and processed by organisations and establishments.
The 1998 Data Protection Act defines data as any information which:

- is processed using equipment operating automatically in response to instructions,
- is recorded with the intention of being processed
- is recorded as part of a relevant filing system
- forms part of an accessible record, including health records

Data Protection under the 1998 Act is about ensuring that personal data about an individual is processed fairly and lawfully in order to protect the rights of an individual.

3. DEFINITIONS OF PERSONAL AND SENSITIVE DATA

- All identifiable members information
- All identifiable donor information
- All identifiable staff information
- Any other identifiable information held on any other person, whether held in electronic or paper form

Certain types of data are regarded as sensitive, and "the Act" stipulates that special measures must be taken in the processing and protection of this type of data.
Sensitive data includes:

- Racial or ethnic origins
- Political opinions
- Religious or similar beliefs
- Membership of trade union
- Physical or mental health condition
- Sexual life
- Any proceedings for any offence or criminal convictions

4. POLICY STATEMENT

The Trust regards the lawful and correct treatment of personal data as crucial to the successful delivery of the highest quality of service. The lawful and correct processing of personal information is a key part of building trust and confidence with external and internal customers. Therefore-

- The Trust will fully implement all aspects of the Data Protection Act 1998.
- The Trust will ensure all staff and other individuals are fully aware of both their rights and obligations under "the Act".
- The Trust will implement adequate and appropriate physical and technical security measures and organisational measures to ensure the security of all information contained in or handled by those systems, including computer systems managed by The Trust, or other agencies on behalf of The Trust.
- It is not the Trust's policy to transfer membership data and the Trust will only transfer personal data outside the European Economic Area (EEA) if the explicit consent of the individual concerned has been given.

5. AIMS OF THE POLICY

The aims of the policy are to fully deliver the Principles as stated in the Data Protection Act 1998.

First Principle:
Personal data shall be processed fairly and lawfully, and in particular, shall not be processed unless specific conditions are met.

Second Principle:
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that or those purposes.

Third Principle:
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Fourth Principle:
Personal data shall be accurate and where necessary, kept up to date.

Fifth Principle:
Personal data shall not be kept longer than necessary, for that purpose or those purposes.

Sixth Principle:
Personal data shall be processed in accordance with the rights of the data subjects in this Act.

Seventh Principle:
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss destruction of, or damage to, personal data.

Eighth Principle:
Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

6. SCOPE OF THE POLICY

The policy covers all aspects of The Trust's business relating to personal information.

The policy covers all methods of holding and storing information including:

- Manually stored paper data, e.g. membership records, donors records, personnel records etc.
- Computer referenced paper data, e.g. databases
- Data held in computer applications and databases
- Data from CCTV and other audio or visual recording systems including tapes
- Data held in records archive storage
- Data held on CD ROMs, floppy disks, computer disks etc.

7. PRACTICAL IMPLICATIONS

Conformance with the Data Protection Act is part of The National Trust for Scotland's duty of confidentiality towards customers, members, donors, staff and other individuals with whom it deals. As general guidance the terms of the Act mean that managers of administrative and support services have a responsibility to ensure compliance with the Act and this policy and also to develop and encourage good information handling practices, within their areas of responsibility. All users of personal data within the Trust have a responsibility to ensure that they process the data in accordance with the eight Principles and the other conditions set down in the DPA.

In particular they will:

- ensure that information is collected, processed, held, transferred and disposed of appropriately, with care for its quality and security
- ensure that the rights of people about whom information is held can be fully exercised under the DPA, including the right to access information.

In addition, the Trust will ensure that:

- staff understand their responsibilities with respect to the proper handling of data through the management, supervision, and training
- there is someone with specific responsibility for data protection in the organisation
- anybody wanting to make enquiries about handling personal information knows what to do and enquiries are dealt with promptly and courteously
- the requirements of the DPA are considered in processes, such as in the development of policy and procedures and the design and the implementation of information systems and the monitoring and evaluation of operational systems and performance
- methods of handling personal information are clearly described and the way personal information is handled and managed is regularly reviewed and audited

In order to meet the requirements of the principles, the Trust will:

- observe fully the conditions regarding the fair collection and use of personal data;
- meet its obligations to specify the purposes for which personal data is used;
- collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements;
- ensure the quality of personal data used;
- apply strict checks to determine the length of time personal data is held;
- ensure that the rights of individuals about whom the personal data is held, can be fully

exercised under the Act;
- take the appropriate technical and organisational security measures to safeguard personal data;
- ensure that personal data is not transferred abroad without suitable safeguards; and
- ensure that all contracts with third parties are data protection compliant

Over time, The National Trust for Scotland will develop an Information Management Framework which will give comprehensive guidance on the handling of confidential/sensitive information.

8. GUIDELINES

a. Individual members of Trust staff must:

- Ensure that they have received training in the handling of personal information;
- Keep all personal information, whether held in electronic or paper format, in a secure environment;
- Ensure that passwords that give them access to personal information are protected and are not disclosed or shared;
- Comply with any published guidance and procedures;
- Not disclose personal information held on others for unauthorised purposes.
- Keep all personal information accurate and up to date
- Dispose of personal information safely and in accordance with the Retention Schedule.

All personal information in the form of manual records should be:

- Kept in a locked filing cabinet: or
- Kept in a locked drawer

If information is computerised, it should be:

- Password protected, with passwords being regularly changed, so that only authorised people can view or alter the data; or
- Kept only on a disk which is itself kept securely in a desk or cabinet to avoid physical loss or damage.

To avoid unauthorised disclosure, care must be taken to site PCs and terminals so that they are not visible except to authorised people. Screens should not be left unattended when personal data is being processed. Similarly, care must be taken to ensure that manual records, e.g. staff or volunteer files, or printouts containing personal data, are not left where they can be accessed by unauthorised staff.

When manual records, or printouts containing personal data, are no longer required, they should be placed into the confidential waste bins to be disposed of securely in accordance with the retention policy.

Particular care must be taken of any data taken away from the organisation, for example manual records to be used at home, or computerised data to use on portable computers or home machines. Where personal data is processed out with the Trust premises all terms of the Data Protection Policy will nevertheless apply. Ensure that all work is kept confidential and, in the case of computerised information, that files are not exposed to risk from virus infection. You should also ensure that all equipment which may contain personal data, e.g. laptops or smart phones, is kept secure at all times and is not exposed to the risk of theft.

Management Guidelines on Data Protection

Managers must:

- Determine if their areas hold personal data and ensure that the data is adequately secure, that access is controlled and that the data is used only for the intended purpose(s).

- Ensure that data protection requirements are observed providing clear messages to their staff regarding appropriate processing of the personal data that they handle.
- Ensure anyone accessing personal data is aware of what the agreed purposes are, and ensure that it is only used for those purposes. Data must not be used for any purpose that we do not have permission to use it for at the time it was collected, unless agreement for additional purposes is obtained.
- Ensure that personal data is not to be distributed or communicated for non authorised purposes. For instance, personal details of a staff member must not be given outside the company without that person's permission; project data containing personal information must not be accessed by someone not directly associated with the project.
- Ensure that personal information must not be transmitted across the internet unless encrypted.
- Ensure that personal information must not be passed to organisations outside of the European Economic area unless certain conditions are satisfied. Contact the Data Protection Officer or Legal Manager for assistance.
- Maintain records of permission or access rights granted to access data . There will be an audit trail to record any changes to personal data
- Record any action taken where personal information is found to be inaccurate. Should someone ask for his or her information to be deleted, a record of this request will be kept along with a record of the action taken.
- Inform the Data Protection Officer of any Data Subject Access requests or Data Protection complaints
- Ensure that all files and data stores will be protected against corruption and accidental loss/damage. In principle, this means having suitable backup and recovery arrangements for the data.
- Identify and address training needs within the team and informing the DPO if the available training will not address those needs.

Confidentiality – Communications

Telephones
Identifiable information is not given over the telephone unless the identity of the requestor has been ensured and they have a genuine reason for requiring access to the data. If possible staff should obtain a land line main switchboard number to confirm the identity of the individual requesting the information. Mobile numbers are not acceptable for purposes of clarification of identity.

Fax Machines
It is good practice to set up pre-set keys with the most regularly used Fax Numbers to reduce the risk of incorrect dialling.

Sending Personal Information by Post
The following guidance should be followed when sending personal information by post:
- Confirm the name, department and address of recipient
- Seal the information in a robust envelope – double envelope or use of robust plastic wallets if appropriate
- Mark the envelope "Private and Confidential"
- Mark the envelope "to be opened by addressee only"
- Send the information by first class post or recorded delivery for staff/volunteer records
- When necessary, ask the recipient to confirm receipt

Clear Desk and Clear Screen
Wherever possible a clear desk policy should be adopted for papers containing person identifiable information to reduce the risk of unauthorised access or loss of and damage to sensitive information outside normal working hours. Information left on desks is also likely to be damaged or destroyed in a disaster such as fire or flood. Screens should be angled away from areas visited by non-employees, and information should be cleared when the user moves away from the workstation. Screen savers should be activated when the user leaves the area and when there is no activity for a short pre-determined time scale. Screen savers should be password protected for reactivation.

Subject Access Request-Rights to Access Information
Employees, donors, members and other people who have personal data held by the organisation have the right to access any personal data that is being kept about them on computer and also have access to paper-based data held in manual filing systems. Any person who wishes to exercise this right should make the request in writing to the Data Protection Officer who will record and forward to the appropriate department. The Trust reserves the right to charge the maximum fee payable for each subject access request. If personal details are inaccurate, they can be amended upon request. The Trust aims to comply with requests for access to personal information as quickly as possible, we are legally obliged to respond to requests within 40 calendar days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request. Failure to comply is a breach of the DPA and the individual could complain to the Information Commissioner.

Third Parties
Where a Third party organisation is engaged to process personal data on behalf of the organisation a contract or written agreement must be formed with the third party, specifying that:

- Personal data will only be processed on the instructions of the National Trust for Scotland
- The third party will put in place appropriate technical and organisational security measures against unauthorised disclosure, unauthorised change, loss and destruction of the data
- The National Trust for Scotland will be permitted to satisfy itself that the technical and organisational security measures are in place and appropriate.

Marketing
Where personal data is used for direct marketing there must be a permission based approach. Individuals should be asked if they are happy for their details to be used for marketing information and to receive news about our products and services. They must be given the opportunity to opt in or opt out of this.

Crime Prevention/Detection
Organisations that have a crime prevention, law enforcement or tax collection function such as the Police, Revenue and Customs or Department of Work and Pensions may require personal information held by The National Trust for Scotland for the prevention or the detection of a crime, apprehend or prosecute an offender or for taxation/ benefit purposes. The National Trust for Scotland may be able to release this information by applying an exemption under Section 29 of the Data Protection Act 1998.
Where disclosure is requested by the police, without exception, the matter should be referred to the Data Protection Officer.

Storage, Retention and Disposal
All data and records should be stored in accordance with the Trust's Records Retention and Management Policy.

9. POLICIES AND PROCEDURES

This policy should be read in conjunction with all National Trust for Scotland policies and procedures including:

- Records and Information Policy
- Records Retention and Management Policy
- Information Security Policies
- Access to Records
- Procurement Policy

10. THE RIGHTS OF THE INDIVIDUAL

Individuals have rights under the terms of the Data Protection Act 1998 in respect of their own personal data held by others.

The National Trust for Scotland will ensure that all individuals are aware of their rights and how to exercise these rights under the Data Protection Act, and will fully comply with the delivery of these rights.

- a right of access to a copy of the information comprised in their personal data;
- a right to object to processing that is likely to cause or is causing damage or distress;
- a right to prevent processing for direct marketing;
- a right to object to decisions being taken by automated means;
- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed
- a right to be informed about the use made of personal data,
- a right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened

11. ROLES AND RESPONSIBILITIES

All Staff
Staff at all levels within The National Trust for Scotland have a responsibility to actively respond to any concerns relating to confidentiality, and ensuring that personal information is processed in accordance with the rights of the individual.

Reporting of Data Protection Incidents
The notification process detailed in Appendix 1 should be adhered to when Data Protection Incidents are identified.

Chief Executive
The Chief Executive has overall responsibility for the implementation and delivery of this Data Protection Policy on behalf of National Trust for Scotland.

The Data Protection Officer/Legal
The Data Protection Officer on behalf of the Chief Executive is responsible for facilitating the implementation of the policy and supporting The National Trust for Scotland staff to understand their responsibilities.

The Data Protection Officer on behalf of the Chief Executive has responsibility for ensuring that The National Trust for Scotland is fully compliant with the rules for notification including:

- that a notification is lodged in its name with the Information Commissioner
- that the notification is lodged within the stipulated time period
- that the notification is concise, correct and maintained
- that any changes are notified within the stipulated time period
- Fee notification

The Data Management Group
The members of the Data Management Group are responsible for overseeing the development of this policy and its implementation. The Data Management Group on behalf of the Trust is also responsible for ensuring the following:

Each individual is aware of his or her rights

- Delivery of staff awareness and training in relation to this policy

The group on behalf of The National Trust for Scotland has a responsibility to ensure that:

- Staff are aware of the policy and of their rights and obligations
- Raising and promoting awareness for staff is an ongoing process

- All individuals managing and handling personal information understand their contractual responsibility for following good data protection practice
- All individuals managing and handling personal information are appropriately trained to do so
- All individuals managing and handling personal information are appropriately supervised
- Individuals are informed of whom to approach if they require assistance and guidance regarding the handling of personal information
- Queries in relation to handling personal information are dealt with promptly and courteously
- Methods of handling personal information are clearly described
- Audits and reviews of procedures in relation to the handling of personal information are undertaken on a regular basis
- Compliance with this policy is regularly assessed and evaluated

Heads of Departments/Operational and Line Managers
All heads of departments and line managers have a responsibility to understand the Act and other related guidance, to establish appropriate procedures to control and manage information and ensure these procedures are followed in compliance with the Data Protection Act 1998.

More detailed guidance will be provided in notes of guidance for staff.

12. Policy Review

This policy will be reviewed annually or in response to legislative or organisational changes.

13. Contact Details

If you have any general enquiries regarding Data Protection please contact:
Internal
Scott McFarlane
The Data Protection Officer
The National Trust for Scotland
5 Cultins Road
Hermiston Quay
Edinburgh
EH11 4DF

External
Information Commissioner - Scotland Office
(Data Protection Act 1998)
28 Thistle Street
Edinburgh
EH2 1EN
Tel: 0131 225 6341
Fax: 0131 225 6989
E-mail: Scotland@ico.gsi.gov.uk
Website: http://www.informationcommissioner.gov.uk

14. GLOSSARY OF TERMS

Personal Data
Personal data means data that relates to a living individual, organised in such a way that the individual can be identified from the data. It includes factual data as well as any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Relevant Filing System

Relevant filing system means that any set of information relating to individuals structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Processing
Processing in relation to information or data, is the obtaining recording or holding of the information or carrying out any operation or set of operations on the information including:

- Acquiring data
- Organising and managing the information or data
- Retrieving and using the information or data by fax, letter, email, or any other means of transmission or dissemination.
- Archiving, disposing of or destroying the information or data.

Data Subject
The Data Subject refers to the individual to whom the personal data relates.

Data Controller
The Data Controller refers to the person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed. The term comprises not only of individuals but also organisations such as companies and other corporate and unincorporated bodies of persons. In the case of The National Trust the Chief Executive is the Data Controller.

Data Processor
The Data Processor refers to any person or organisation (other than an employee of the data controller) who processes data (including storage or otherwise managing) the data on behalf of the data controller.

Recipient
The recipient refers to any person or organisation to which data are disclosed but does not include any person to whom disclosure is made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.

Third Party
Is any legal entity or person who is not the data controller (including other companies in the same group)

Opt In
Is a statement that notifies the individual of the uses to which data will be put and asks the individual to actively agree to those uses. There is usually a tick box, which should not be pre-ticked. If the individual does tick the opt-in box they are giving consent for their data to be used.

Opt – out
Is a statement that notifies the individual of the uses to which data will be put and asks the individual to object if they disagree. If the statement is in written or electronic form there is usually a tick box. If the individual does not tick the box they give their consent to the uses stated.

Consent
This is a freely given, specific and informed indication of wishes by which the Data Subject signifies agreement to personal data being processed. In the direct marketing industry, consent to process is normally achieved by coupling this requirement by an opt-out or an opt-in statement to provide the Data Subject with an opportunity to prevent direct marketing approaches.

Subject Access Request
This is a written, signed request from an individual to see information held on them. The Data Controller must provide all such information in a readable form within 40 days of receipt of the request and may charge a fee of up to £10.

Privacy Policy
This is a publicly available document that outlines a company's intentions concerning personal data storage and use.

Electronic Mail
Any text, voice, sound, or image message sent over a public electronic communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient and includes messages sent using a short message service.

15. European Economic Area (EEA)
The European Economic Area refers to the following European countries or territories:
Austria
Belgium
Bulgaria
Cyprus
Czech Republic
Denmark (excluding the Faroe Islands)
Finland
France
Germany
Gibraltar
Greece
Hungary
Iceland
Ireland
Italy
Latvia
Liechtenstein
Lithuania
Luxembourg
Malta
Netherlands
Norway
Poland
Portugal
Romania
Slovak Republic
Slovenia
Spain
Sweden
United Kingdom (excluding Isle of Man and the Channel Islands)

Appendix 1

Data Protection Incident Reporting Structure for an identified Data Protection Incident