Data Protection Policy V2.0

Document Control

Title	Data Protection Policy
Author	Head of Information Governance
Approved by	HES Board
Date of Approval	16/11/2015
Version Number	2.0
Review frequency	Annually for the first 2 years from approval, then every 2 years or at change of legislation.
Next review date	January 2018

Version Control

Version	Date	Status	Prepared by	Amendments
0.1	15 October 2014	Draft	D Paris	
0.2	22 October 2014	Draft	D Paris	Minor changes from comments
0.3	28 September 2015	Draft	D Paris	Changes after input from external consultants
0.4	12 October 2015	Draft	D Paris	Minor updates from TUA Consultation.
1.0	17 November 2015	Approved	D Paris	Approved by HES Board 16/11/2015
2.0	11 January 2017	Approved	D Paris	No significant amendments to policy made. Updated DPO contact details No additional approval required

Contents

1. Introduction

Through its day to day operations Historic Environment Scotland (HES) is required to collect, use and retain certain types of personal data about a variety of individuals. These include customers, suppliers, current, past and prospective employees, volunteers, members, historic property owners, donors, potential donors and others with whom it communicates.

To protect the privacy of those individuals, HES is required by law to comply with the Data Protection Act 1998 (DPA). The Act came into force on 1st March 2000 and establishes a framework of rights and duties which balance the need of organisations to collect and process personal data for clearly defined purposes with the right of the individuals to confidentiality. These individuals are known as data subjects under the Act.
This policy helps to protect HES and its data subjects from some very real data security and privacy risks, including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately
- **Failing to offer choice**. For instance, all individuals should be free to choose how HES uses data relating to them
- **Reputational damage**. For instance, HES could suffer if hackers successfully gained access to sensitive data

Compliance with the DPA is not just a statutory obligation. HES regards the lawful and correct treatment of personal information as of vital importance to maintaining trusted and positive working relationships with the various groups of individuals whose personal data HES holds and to successful business operations.

2. Purpose

The purpose of this policy as well as related procedures and guidance is:

- to set out HES' obligations under the DPA for fair and lawful processing of personal data in the records created and received in the course of its activities;
- to demonstrate its commitment to and compliance with the DPA and related legislation and standards that govern the privacy of individuals with whom HES has a relationship.

3. Scope

The DPA relates to the processing of personal data. Personal data is factual information that both identifies and relates to a living individual, and includes any expression of opinion about the individual.

The DPA categorises some types of personal data as "sensitive personal data" to which stricter conditions apply. This includes personal data concerning racial or ethnic origin, political or religious beliefs, trade union membership, physical or mental health, sexual orientation and criminal records.

The majority of the personal data held by HES is not sensitive and is made up of data provided by employees and stakeholders.

The policy is applicable to all HES employees, volunteers, contractors, service providers and other organisations working for or on behalf of HES.

The policy applies to all personal data regardless of format or medium, including paper, electronic, audio, visual, microfilm and photographic.

4. Policy Statement and Commitment

In order to fulfil its obligations under the DPA, HES is committed to complying with the eight data protection principles set out in Schedule 1 of the Act:

1. Personal data shall be processed fairly and lawfully
2. 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 purpose or those purposes
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Personal data shall be accurate and, where necessary, kept up to date
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
6. Personal data shall be processed in accordance with the rights of data subjects under this Act
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8. 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

To comply with the DPA principles, HES is committed to the following policy statements and related business practice, procedures, processes and systems.

4.1 Registration

HES is registered with the Information Commissioner's Office as a Data Controller: Reference (ZA143443) and has an entry in the Data Protection Register.[1]

The HES DPA register entry has information on the following:

- the class(es) of personal data held;
- the purpose(s) for which data are held;
- the source(s) from which data are obtained ;
- people or organisations to whom we may disclose the data ;
- any countries overseas to which we may transfer the data

HES is required to ensure that its entry in the Register is correct and up to date. The Data Protection Officer must be informed immediately if a new work process or project will involve the need to hold, process or disclose information in a manner at variance with the HES register entry. The registration requires renewal on an annual basis.

[1] ICO Register, https://ico.org.uk/ESDWebPages/DoSearch?reg=648605, accessed 11/01/2017

4.2 Fair and lawful processing and purpose

HES collects and processes appropriate personal information only to the extent that it is required to fulfil operational need or to comply with any legal requirement.
HES uses privacy notices to inform the data subject wherever collection of personal information takes place, outlining the purpose for which it will be used, who it will be shared with, how it will be securely retained and how individuals may access it.

HES seeks explicit consent from its data subjects when collecting sensitive information, collecting personal data for unexpected or potentially objectionable purposes, processing information in a way which may significantly affect an individual, or sharing information with another organisation which would be unexpected;

Related docs: *Privacy notices*

4.3 Adequate and Accurate Data

All employees who work with personal data will take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets
- HES will make it easy for data subjects to update the information HES holds about them

All employees are responsible for:

- checking that any personal information that they provide in connection with their employment is accurate and up to date;
- informing the HR Department of any changes to information that they have provided, i.e. changes of address ;
- informing the HR Department of any errors or changes.

4.4 Data Retention & Disposal

HES retains personal data only for as long as they are needed through the maintenance and application of retention and disposal schedules and confidential disposal procedures for all HES information.

Related docs: *Retention Schedules, Disposal Procedures*

4.5 The Rights of Data Subjects

HES ensures that people about whom it holds information can exercise their rights fully under the Act.
All HES Data Subjects are entitled to know:

- what personal information HES holds and processes about them and why;
- how to gain access to it;
- how to keep it up to date or correct it;
- what HES is doing to comply with its obligations under the DPA.

A DPA statement is provided whenever personal data is gathered (for example, on a form) explaining why the data is required, and how it will be used.

4.6 Subject Access Requests (SARs)

SARs are requests to HES for personal data made by the data subject. In some cases, a SAR may be made by a third party on that person's behalf, e.g. by

- a parent on behalf of a young child
- a representative on behalf of an adult with incapacity
- a solicitor on behalf of a client.

HES takes reasonable steps to make sure that the person making the SAR is who they say they are. If someone is making a request on behalf of a third party, HES checks that they have the authority to make that request.

Requests for access to personal data (other than those falling within routine business) should be addressed in writing or email to the Data Protection Officer, ideally using the HES Subject Access Request form which is available via the website or in hard copy on request. A fee of £10 will normally be payable.

HES aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 calendar days as required in the Act unless there is a good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

Related docs: *Subject Access Request Procedure*; *Subject Access Request Form*

4.7 Data Security

HES takes appropriate technical and organisational security measures to safeguard personal information and has established information security procedures for both manual and electronic records, subject to appropriate risk assessment.

All staff are responsible for ensuring that:

- any personal data that they hold, whether in Electronic or Paper format, is kept securely ;
- personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Related docs: *Information Security Policy and Procedures*

4.8 Breaches and Near Misses

HES has procedures in place to identify and respond to compliance breaches and near misses. These **must be reported immediately** to the DPO (in whose absence, the Senior Information Risk Owner, which failing another member of the senior management team).

Related doc: *Responding to data compliance breaches and near misses*

4.9 Data Processors

Where HES uses a contractor to process personal data on its behalf (a "data processor"), HES must be satisfied that the contractor is taking adequate steps to allow HES to meet its

obligations under the DPA. Contracts between HES and data processors must ensure that all necessary security procedures and other appropriate measures are specified in the contract, and the contract must be monitored to ensure that they are being adhered to.

4.10 Sharing Personal Data

HES will not disclose personal data to any third party unlawfully.

Where and when appropriate, HES will share information in line with the Information Commissioner's Data Sharing Code of Practice and establish Data Sharing Agreements with third parties, outlining the terms under which information will be shared.

Related docs: *Data Sharing Agreement with Historic Environment Scotland Enterprises Ltd.*

4.11 Use of personal data for research, statistical or historical purposes

HES informs individuals of their responsibilities when using personal data for research, statistical or historical purposes, for example, onsite researchers accessing search rooms, and asks them to confirm that they will abide by these terms of access and use.

Related docs: *Research Use of Personal Data in Historic Environment Scotland fact sheet & procedure*

4.12 Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject, for example CCTV footage required for a criminal investigation.

Under these circumstances, HES will disclose requested data. However, as a data controller the organisation will ensure the request is legitimate, seeking assistance from the company's legal advisers where necessary.

4.13 Privacy by Design

HES is committed to taking a pro-active approach to privacy and data protection.

- core privacy considerations are integrated into existing project management and risk management methodologies and policies.
- Privacy impact assessments are used to identify and reduce the privacy risks of any planned changes within the organisation

4.14 Regulator Engagement

HES will engage the Office of the Information Commissioner directly in policy and process discussions touching on privacy, data sharing and other data protection issues.

4.15 Training

HES provides role-based training for all HES employees in information management, security, governance and compliance, to ensure that every member of staff understands their responsibility under the Act.

Related docs: *Training Programme*

5. Roles and Responsibilities

5.1 All staff

Compliance with this Policy is the responsibility of all HES employees and everyone who has access to HES records. Breaches of this policy and therefore the Act, whether deliberate or through negligence, may lead to disciplinary action, in line with HES disciplinary procedures. A breach of the Act could also lead to criminal prosecution.

Colleagues must familiarise themselves with, and follow, this policy as well as the supporting codes of practice, ensure that procedures for the collection and use of personal data is complied with in their area, and familiarise themselves with the implications of data protection in their job.

5.2 Chief Executive

HES is the Data Controller under the Act and the Chief Executive has senior management responsibility for ensuring that all collection and processing of personal data within the organisation complies with the Act and its principles.

5.3 Data Protection Officer

The HES Data Protection Officer (DPO), who is the named contact for all Data Protection issues, is the Data Protection and Freedom of Information Manager, 0131 668 8713, dataprotection@HES.scot

The DPO must ensure that

- the HES Data Protection Notification, Data Protection Policy, Data Protection Code of Practice: Archive Collections, Surveillance Camera Code of Practice & Privacy Impact Assessment Guidance is kept up to date
- identify and publicise responsibilities for Data Protection within HES
- support all members of staff to comply with their obligations under the Act
- issue guidance and training
- monitor and report on the proper functioning of data protection systems.

5.4 Senior Management

Senior management will make provision for a regular review of this policy and investigate modifications when necessary.

5.5 Heads of Department and Line Managers

Heads of Department and line managers have day-to-day responsibility for ensuring compliance with the Act within their area of responsibility. To fulfil this responsibility they must:

- ensure that personal data held by their department is kept securely and used properly, within the terms of the Act
- inform the Data Protection Officer of the types of personal data held in their department, and any changes or new holdings. (The Data Protection Officer will advise on the implementation of the Act.)
- keep the Data Protection Officer informed of changes in the collection, use, and security of Personal Data within their department.

- ensure that appropriate technical and organisational measures are taken within their department to prevent unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, such data
- ensure that staff with specific data protection responsibilities have these written into their job descriptions and fulfil their data protection responsibilities properly
- ensure that all staff receive the data protection training provided.

5.6 Information and Information Systems Governance Board

Information and Information Systems Governance Board (IISGB) will review all Policy and Procedures relating to Data Protection and supply a relevant recommendation to the HES Board.

The IISGB will review all data breach reports and, where appropriate, make a recommendation to the HES Board.

The IISGB will also ensure the Data Protection Policy and associated procedures are reviewed in line with agreed review dates and any changes to legislation.

5.7 Historic Environment Scotland Board

The HES Board has the responsibility for adopting best practice as an employer and public body, including review and approval of Data Protection Policy and related procedures, on the recommendation of the Chief Executive and the IISGB.[2]

6. Legislative Framework

Compliance with this policy will facilitate compliance with the following acts, regulations and standards.

- Data Protection Act 1998
- Human Rights Act 1998
- Freedom of Information (Scotland) Act 2002
- Environmental Information Regulations (Scotland) 2004
- Privacy and Electronic Communications Regulations 2003
- Surveillance Camera Code of Practice
- Payment Card Industry (PCI) Data Security Standard 3.1
- Statistics and Registration Service Act 2007
- Equality Act 2010
- Public Records (Scotland) Act 2011
- HES operates in accordance with HMG Security Policy Framework, HMG Information Assurance (IA) standards and their associated Good Practice Guides / Supplements / IA Notices.
- HES also aims to operate in accordance with the following best practice standards for security and recordkeeping:
    - BS ISO 27001: 2005 - Information Technology - Security Techniques
    - BS EN 15713: 2009 – Secure Destruction of Confidential Material
    - BS ISO 15489: 2001 – Information & Documentation – Records Management (Parts 1 & 2)

[2] Historic Environment Scotland, Scheme of Internal Delegation September 2015.

7. Relationship to other HES Policies

This policy forms part of HES's overall policy framework but specifically relates to the following policies and procedures:[3]

- Data Protection Code of Practice: Archive Collections
- Information Security Policy
- Security Incident Reporting Procedure
- Records Disposal Policy
- Data Handling and Management Policy
- Retention and Disposal Schedule
- Surveillance Camera Code of Practice

8. Monitoring and Review

This policy and associated training will be reviewed at least every two years in order to take account of any new or changed legislation, regulations or business practices.

The regular monitoring, review and audit of the way in which personal information is collected, stored and used by HES will be coordinated by the Head of Information Governance in consultation with the Chief Executive.

[3] Others will be added as the Policy Framework for Historic Environment Scotland develops.