Data Protection Policy V3.0

Document Control

Title	Data Protection Policy
Author	Head of Information Governance
Version Number	3.0
Review frequency	Annually for the first 2 years from May 2018, then every 2 years or at change of legislation.
Next review date	May 2019

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 2018	Approved	D Paris	No significant amendments made to policy. Updated DPO contact details. No additional approvals required.
2.1	7 February 2018	Draft	D Paris	Amendments for GDPR
2.2	16 February 2018	Draft	D Paris	Formatting and structural amendments as part of GDPR review
2.3	15 March 2018	Draft	D Paris	Updated with comments from Director of Finance and Performance
3.0	25 April 2018	Final	D Paris	Approved by ARAC

Table of Contents

1. Introduction

1.1. Through its day to day operations Historic Environment Scotland (hereafter '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.

1.2. To protect the privacy of those individuals, HES is required by law to comply with the General Data Protection Regulation (hereafter 'GDPR'). The GDPR was approved by the EU Parliament on 14 April 2016 and is enforceable from 25 May 2018. It is designed to standardise data privacy laws throughout the EU to ensure a consistent approach to all EU citizens' data privacy. The GDPR 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.

1.3. This policy helps to protect HES and its Data Subjects from 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

1.4. Compliance with the GDPR is not just a statutory obligation. HES regards the lawful and correct treatment of Personal Data 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

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

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

3. Scope

3.1. The GDPR 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.

3.2. The GDPR classifies some types of Personal Data as “Special Category” 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.

3.3. The majority of the Personal Data held by HES is not part of the Special Category Data and is made up of data provided by employees and stakeholders.

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

3.5. 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

4.1. In order to fulfil its obligations under the GDPR, HES is committed to complying with the six data protection principles.

4.2. Article 5 of the GDPR requires that Personal Data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the

appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

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

5. The Rights of the Data Subject

5.1. HES ensures that Data Subjects can fully exercise their rights under the GDPR.

5.2. The GDPR provides the following rights for Data Subjects

5.2.1. The Right to be Informed

a. 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.

b. HES uses privacy notices to inform the Data Subject wherever collection of Personal Data takes place, outlining the legal processing condition, the purpose for which it will be used, who it will be shared with, how it will be securely retained, how long it will be kept for and how individuals may access it.

c. HES seeks consent from its Data Subjects when collecting Special Category Data, 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.

d. A data protection 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.

5.2.2. The Right of Access

a. Subject Access Requests (hereafter ‘SAR’) are requests, made by the Data Subject, to access their Personal Data held by HES. In some cases, a SAR may be made by a third party on that Data Subject’s behalf, e.g. by

i. a parent on behalf of a young child.
ii. a representative on behalf of an adult with incapacity.
iii. a solicitor on behalf of a client.

b. 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.

c. 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.

d. HES aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 28 calendar 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.

5.2.3. The Right to Rectification

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

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

b. All employees are responsible for

    i. checking that any Personal Data that they provide, in connection with their employment, are accurate and up to date;
    ii. informing the Human Resources Department of any changes to their Personal Data they have provided, i.e. change of address; and
    iii. informing the Human Resources Department of any errors in their Personal Data.

5.2.4. The Right to Erasure

a. 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.

b. The right to erasure does not provide an absolute right to be forgotten. Data Subjects have the right to have Personal Data erased or prevent further processing under certain conditions.

    i. Where the Personal Data is no longer required for the purpose it was originally collected for.
    ii. When the Data Subject withdraws consent, where consent was the legal processing condition.

iii. When the Data Subject objects to processing and there are no overriding, legal reason for continuing to process the Personal Data.
iv. The processing was unlawful to begin with.
v. The Personal Data has to be erased in order to comply with a legal obligation.
vi. The Personal Data is processed in relation to supplying 'information society services' to children.[1]

c. HES can refuse the right of erasure under the following circumstances.

i. When complying with a legal obligation for the performance of a public task or exercise of official authority.
ii. For public health purposes in the public interest.
iii. The exercise or defence of legal claims.
iv. When archiving or adding to the National Record in the public interest, scientific or historical research or statistical purposes.
v. When exercising the right of freedom of information or expression.

5.2.5. The Right to Restrict Processing

a. Data Subjects have the right to restrict, block or supress the processing of Personal Data. When processing is restricted, HES is permitted to retain the Personal Data but no further processing must take place.

b. HES will restrict processing in the following conditions.

i. Where the accuracy of the Personal Data is contested by the Data Subject. Processing will be restricted until the accuracy of the Personal Data has been verified.
ii. Where the processing has been objected to by the Data Subject and the processing was on the basis of performance of a public task. Processing will be restricted whilst HES considers the whether the legitimate grounds override the rights of the Data Subject.
iii. When the processing was unlawful and the Data Subject requests restriction rather than erasure.
iv. When HES no longer requires the Personal Data but the Data Subject required the Personal Data to be retained to establish, exercise or defend a legal claim.

5.2.6. The Right of Data Portability

a. Data Portability allows a Data Subject to obtain their Personal Data to reuse across different services. It allows the moving, copying or transferring of their

[1] Article 1 Point 2 of Directive 98/48/EC describes an Information Society Service as any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services, https://publications.europa.eu/en/publication-detail/-/publication/695afd1d-539b-4475-a892-d1f5bbc9f489/language-en, accessed 16/02/18.

Personal Data from one IT system to another in a safe and secure manner. The right of data portability only applies

i. to personal data a Data Subject has provided to HES;
ii. where the legal processing condition is consent or for the performance of a contract; and
iii. when the processing is carried out by automated means.

5.2.7. The Right to Object

a. Data Subjects have the right to object to processing based on legitimate interests, performance of a task in the public interest, direct marketing, profiling and for the purposes of historical or scientific research and statistics. HES will stop processing unless

i. HES can demonstrate compelling legitimate grounds which override the rights of the Data Subject; and
ii. the processing is for the establishment, exercise or defence of legal claims.

5.2.8. Rights Related to Automated Decision Making including Profiling

a. The GDPR applies to all automated decision making and profiling processing.

6. Data Security

6.1. 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.

6.2. All staff are responsible for ensuring that:

- Any Personal Data that they hold, no matter the format, is held securely; and
- Personal Data is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party.

7. Breaches and Near Misses

7.1. HES has procedures in place to identify and respond to compliance breaches and near misses. These must be reported immediately to the Data Protection Officer or the Head of Information Governance, in whose absence, to the Senior Information Risk Owner failing that another member of the Senior Management Team.

8. Data Processors

8.1. Where HES uses a contractor to process Personal Data on its behalf, HES must be satisfied that the contractor is taking adequate steps to allow HES to meets its obligations under the GDPR.

8.2. Contracts between HES and the Data Processor must ensure that all necessary security procedures and other appropriate measures are specified in the contract, and that the contract must be monitored to ensure that they are being adhered to.

8.3. HES uses a Third Party Security Questionnaire as part of its official procurement process when tendering for goods or services which may involve the processing of Personal Data by a Data Processor.

9. Sharing Personal Data

9.1. HES will not disclose Personal Data to any third party unlawfully.

9.2. 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.

10. Use of Personal Data for Research, Statistical or Historical Purposes

10.1. 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 the terms of access and use.

11. Disclosing Personal Data for Other Reasons

11.1. In certain circumstances HES may release Personal Data to law enforcement agencies without the consent of the Data Subject, for example, CCTV footage required for a criminal investigation.

11.2. As Data Controller, HES will comply with the Surveillance Camera Code of Practice and will ensure that all requests from law enforcement agencies are legitimate, seeking advice from legal advisers where required.

12. Privacy by Design

13.1. 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

13. Regulator Engagement

14.1. HES will engage, as appropriate, with the Information Commissioner's Office directly in policy and process discussions touching on privacy, data sharing and other data protection issues.

14. Training

15.1. HES provides eLearning and classroom based training for all HES employees in information management, security, governance and compliance, to ensure that every member of staff understands their data protection responsibilities when using Personal Data.

15. Roles and Responsibilities

15.1. All Staff

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

15.1.2. 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.

15.2. Chief Executive

15.2.1. HES is the Data Controller under the GDPR and the Chief Executive has senior management responsibility for ensuring that all collection and processing of Personal Data within HES complies with the GDPR and its principles.

15.3. Head of Information Governance

15.3.1. The Head of Information Governance ensures that all data protection and information security related policies and procedures are kept up to date. They monitor and report on the proper functioning of data protection systems and will liaise with the Chief Executive on all matters relating to the protection of Personal Data and the privacy of HES' Data Subjects.

15.3.2. The Head of Information Governance is also the Data Protection Officer for HES, 0131 668 8771, dataprotection@hes.scot.

15.3.3. The Data Protection Officer must ensure that

a. the HES Data Protection Notification, Data Protection Policy, Data Protection Code of Practice: Archive Collections and Business Information is kept up to date
b. identify and publicise responsibilities for Data Protection within HES
c. support all members of staff to comply with their obligations under the Act
d. issue guidance and training
e. monitor and report on the proper functioning of data protection systems.

15.4. Senior Management

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

15.5. Head of Department and Line Managers

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

a. ensure that Personal Data held by their department is kept securely and used properly, within the terms of the GDPR;
b. 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 GDPR.);
c. keep the Data Protection Officer informed of changes in the collection, use, and security of Personal Data within their department;
d. 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;
e. ensure that staff with specific data protection responsibilities have these written into their job descriptions and fulfil their data protection responsibilities properly;
f. ensure all staff complete their mandatory Data Protection and Information Security Awareness training.

15.6. Historic Environment Scotland Board

15.6.1. 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 Senior Management Team and the Chief Executive.[2]

[2] Historic Environment Scotland, Scheme of Internal Delegation September 2017.

16. Legislative Framework

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

a. General Data Protection Regulations
b. Human Rights Act 1998
c. Freedom of Information (Scotland) Act 2002
d. Environmental Information Regulations (Scotland) 2004
e. Privacy and Electronic Communications Regulations 2003
f. Surveillance Camera Code of Practice
g. Payment Card Industry (PCI) Data Security Standard 3.1
h. Statistics and Registration Service Act 2007
i. Equality Act 2010
j. Public Records (Scotland) Act 2011
k. Digital Economy Act 2017
l. HES operates in accordance with HMG Security Policy Framework, HMG Information Assurance (IA) standards and their associated Good Practice Guides / Supplements / IA Notices.
m. 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)