ARCHAEOLOGY SCOTLAND

Personal Data Protection Policy

Title	Personal Data Protection Policy
Responsible person	Eila Macqueen, Data Manager (not DPO)
Review frequency	Annually for the first 2 years from May 2018, then every 2 years or at change of legislation
Policy approved	Approved by Board on 3rd July 2018
Next review	May 2019

Table of Contents

1. Introduction

1.1 Through its day to day operations Archaeology Scotland (hereafter 'AS') is required to collect, use and retain certain types of Personal Data about a variety of individuals. These include suppliers, current, past and prospective employees, volunteers, members and associates, potential members and others with whom it communicates.

1.2 To protect the privacy of these individuals, AS as the Data Controller 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 fully absorbed into UK law through the Data Protection Act 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 AS 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 AS uses data relating to them
- Reputational damage. For instance, AS could suffer if hackers successfully gained access to sensitive data

1.4 Compliance with the GDPR and Data Protection Act 2018 is not just a statutory obligation. AS 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 AS 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 AS 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 AS 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 AS 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 AS employees, volunteers, contractors, service providers and other organisations working for or on behalf of AS.

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, AS as the Data Controller 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 GDPR principles, AS is committed to following the policy statements and related business practice, procedures, processes and systems.

4.4 AS is committed to privacy by design and taking a pro-active approach to privacy and data protection.

4.5 To ensure its processing of data is lawful, fair and transparent, AS maintains a Register of Data Processing Activities, which notes the legal basis for all data processing.

4.6 The Register of Data Processing Activities is reviewed at least annually.

5. The Rights of the Data Subject

5.1 AS 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) AS collects and processes appropriate personal information only to the extent that it is required to fulfil operational needs or to comply with any legal requirement.
b) AS uses privacy notices to inform the Data Subject wherever collection of Personal Data takes place, outlining the legal basis for processing, what data is collected and the purpose for processing, who it will be shared with, and how long it will be retained.
c) AS 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 AS.
b) Requests for access to Personal Data should be addressed in writing or email to the Data Manager.
c) AS aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 28 calendar days 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.
d) If someone is making a request on behalf of a third party, AS checks that they have the authority to make that 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. AS will make it easy for Data Subjects to update their Personal Data.
    ii. Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
    iii. Regular updates of Personal Data are carried out as specified in the Register of Data Processing Activities.
b) All employees are responsible for:
    i. checking that any Personal Data that they provide, in connection with their employment, is accurate and up to date;
    ii. informing the Office Manager of any changes to their Personal Data, i.e. change of address, emergency contact; and
    iii. informing the Office Manager of any errors in their Personal Data.

5.2.4 The Right to Erasure

a) AS retains Personal Data only for as long as it is needed for the stated purpose at point of collection, through the implementation of retention policies and disposal procedures. For details, see AS Data Retention Policy.
b) Data Subjects have the right to have Personal Data erased or prevent further processing under certain conditions (see ICO guidance for more information). The right to erasure does not provide an absolute right to be forgotten.

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, AS is permitted to retain the Personal Data but no further processing must take place.
b) AS 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 Processing will be restricted whilst AS considers 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 AS 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 Personal Data from one IT system to another in a safe and secure manner.
b) The right of data portability only applies
    i. to personal data a Data Subject has provided to AS;
    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. AS will stop processing unless
    i. AS 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) Data Subjects can object to potentially damaging decision being taken against them based only on automated data processing.

6. Data Security

6.1 AS 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 AS ensures that

a) personal data stored electronically is secure, using up-to-date software.
b) access to personal data is limited to personnel who need access and appropriate security is in place to avoid unauthorised sharing of information
c) personal data is deleted securely, such that the data is irrecoverable
d) appropriate back-up and disaster recovery solutions are in place.

6.3 All staff are responsible for ensuring that:

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

7. Data Breaches

7.1 AS has procedures in place to detect and respond to personal data security breaches (see AS Personal Data Breach Policy). Any breaches must be reported immediately to the Director or Data Manager, in whose absence, to the Office Manager.

8. Data Processors

8.1 Where AS uses a contractor to process Personal Data on its behalf, AS must be satisfied that the contractor is taking adequate steps to meet its obligations as the Data Processor and allow AS to meet its obligations at the Data Controller under the GDPR.

8.2 Contracts between AS and the Data Processor must ensure that all necessary security procedures and other appropriate measures are specified in the contract.

9. Sharing Personal Data

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

9.2 Where and when appropriate, AS 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.

9.3 If legally required, AS may release Personal Data to law enforcement agencies without the consent of the Data Subject.

10. Training

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

11. Roles and Responsibilities

11.1 All Staff

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

11.1.2 Colleagues must familiarise themselves with, and follow, this policy as well as the supporting policies, 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.

11.2 Director

11.2.1 AS is the Data Controller under the GDPR and the Director has senior management responsibility for ensuring that all collection and processing of Personal Data within AS complies with the GDPR and its principles.

11.3 Data Manager

11.3.1 The Data Manager is responsible for ensuring AS, its employees and representatives adhere to and comply with the Data Protection legislation and relevant codes of practice. They will also monitor and check compliance. More specifically the AS Data Manager has, but is not limited to, the following responsibilities:

a) ensure that AS, its employees and representatives adhere to this policy
b) ensure that AS, its employees and representatives adhere to the six principles of the GDPR
c) ensuring that AS employees and representatives have regular refresher courses on the data protection principles and how to apply them
d) ensure that all personal information is handled with respect
e) ensure that retained personal information is secure, relevant and not retained for any time longer than is necessary for the purpose for which it was acquired
f) annual data audit and review of the Register of Data Processing Activities
g) monitor changes to systems and documentation to ensure compliance with the Data Protection legislation and codes of practice
h) ensure compliance with any Subject Access Request that is received.

11.4 AS Board

11.4.1 The AS Board has the responsibility for adopting best practice as an employer and third sector body, including review and approval of Data Protection Policy and related procedures, on the recommendation of the Director and the Data Manager.