Scottish Wildlife Trust

Data Protection

Retention and disposal policy

1. Introduction

The Trust's Retention and Disposal Policy details how we will retain and dispose of information in order to ensure consistently across the organisation.

Data is stored in a number of areas throughout the Trust, including servers (central or held by third parties), email accounts, workstations, backups and paper files.

Data subjects will be informed of the retention period, or if no fixed retention period can be provided – the criteria used to determine that period.

2. General retention periods

Personal data should only be retained for as long as necessary to meet the Trust's needs, together with legal and regulatory requirements (e.g. tax law, employment law, companies act).

In the absence of any legal requirements, personal data may only be retained as long as necessary for the purpose of processing. Data must be deleted when, for example:

- the data subject has withdrawn consent to processing;
- a contract has been performed or cannot be performed anymore; or
- the data is no longer up to date.

Where records are likely to have a historical value or are worthy of permanent preservation, they will be archived.

During the retention period, the data owner will regularly review data to ensure it is kept up to date and is being processed in line with the legal grounds for processing.

3. Disposal schedule

Information will have agreed disposal schedules such as: destroy after an agreed period; permanently preserve; or keep under review, to determine whether data should be destroyed, retained for a further period or transferred to an archive for permanent preservation.

After the expiration of the relevant retention period, personal data should either be securely destroyed or anonymised.

4. Anonymisation or destruction

Anonymisation can be achieved by:

- erasing unique identifiers within the data set;
- erasing pieces of information that identify the data subject;
- separating personal data from non-identifying information; or
- aggregating personal data so no allocation to an individual is possible.

In some cases, no action will be required if data cannot be allocated to an identifiable person at the end of the retention period.

When data is no longer required it should be securely destroyed. Records can be destroyed in the following ways:

- non-sensitive information – placed in a normal rubbish bin
- confidential information – cross cut shredded or confidential waste bags
- electronic equipment containing information – destroyed via ICT Manager to ensure completely non-recoverable.

5. Information sharing

Duplicate records should be destroyed. Where information has been regularly shared between functions, only the original records should be retained. Take care to ensure that seemingly duplicate records are handled correctly.

6. Retention timescales

Where the records fall into categories listed on the information retention schedule no documentation is required. Data disposed of outwith this schedule will need to be recorded.