DATA PROTECTION POLICY

Approved by the Board of Trustees, May 2026

1 - INTRODUCTION

Related policies include

- Data retention, archiving & destruction policy,
- Whistleblowing policy,
- IT & managed devices policy, including Acceptable Use of IT, Cyber Security Policy & Work Mobile Devices Policy.

Purpose and scope

Suffolk Wildlife Trust is committed to protecting the rights and freedoms of individuals with respect to the processing of personal data.

This policy sets out how we comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

We ensure that personal data is:

- Processed lawfully, fairly and transparently
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Retained only as long as necessary
- Processed securely

This policy applies to:

- All employees
- Contractors and consultants
- Temporary staff
- Volunteers
- Anyone processing personal data on behalf of the organisation

It applies to all personal data processed by the organisation, whether held electronically on paper, or other formats.

All third parties working with, or for the Trust who have or may have access to personal data are required to read, understand, and fully always comply with this policy. All third parties are required to enter into a data processor or data sharing agreement prior to accessing or processing any personal data.

Staff who supervise volunteers in roles who may be exposed to large amounts of personal data must ensure the volunteers read this policy in addition to reading and signing the Volunteer Data Protection.

2 - LEGAL FRAMEWORK

2.1 Data Protection legislation

In order for the Trust to fulfil its charitable purpose, it collects and processes information about its staff, volunteers, members, donors, customers, contractors and partners.

Indicatively, the Trust collects and uses personal data for the purposes of:

- Administration of memberships, donations and fundraising
- Marketing and communications about our work, events and programmes
- Fulfilment of contracts with clients and suppliers
- Recruitment and employment
- Fulfilling our duties as an accredited training centre

The UK GDPR and Data Protection Act 2018 govern the processing of personal data of living persons. The purpose of the legislation is to safeguard the rights and freedoms of individuals whose personal data is being processed by the Trust. In particular it provides for the collection and use of personal data in a responsible way, whilst protecting against unwanted or harmful uses of personal data.

The Trust is a Data Controller relying on multiple lawful bases for the processing of personal data (lawful basis for each specific processing activity is detailed in the Trust's Record of Processing Activities (ROPA).

2.2 Principles relating to the processing of personal data

The Trust is responsible for meeting all relevant requirements and must be able to demonstrate compliance with the principles of data protection.

These are as follows:

i. **Lawfulness, fairness and transparency**
Personal data shall be processed lawfully, fairly and in a transparent manner. The Trust will obtain and process personal data fairly in accordance with the fulfilment of the functions conferred upon it. The Trust will ensure a Data Protection and Privacy Notice is provided at the point at which personal data is collected and will be available on the website.

ii. **Purpose limitation**
Personal data shall be collected only for specified, explicit and legitimate purposes communicated at the time of collection. The Trust will process data which has been collected only in ways compatible with these purposes.

iii. **Data minimisation**
Personal data processed by the Trust will be adequate, relevant and not excessive to the purpose(s) for which it was collected. The Trust aims to process as little personal data as possible.

iv. **Accuracy**
Personal data shall be accurate, complete and up-to-date. The Trust will implement procedures which are adequate to ensure high levels of data accuracy, including the necessary supporting systems and staff training.

v. **Storage limitation**
Personal data shall only be retained for as long as it is necessary to do so. The Trust has implemented retention periods for the storage of personal data as set out in its *Data retention, archiving & destruction policy*. Staff are required to be familiar with this approved schedule. Where a member of staff has any queries, they should contact their manager.

vi. **Integrity and confidentiality**
Personal data shall be processed in an appropriate manner to maintain the security of the dataset. The Trust will take appropriate security measures against unauthorised access to, alteration, disclosure, or destruction of the personal data against their accidental loss or destruction. The Trust commits to ensuring that high standards of security are maintained at all times when dealing with personal data by the implementation of appropriate technical and organisational measures.

vii. **Accountability**
The Trust will demonstrate its compliance with data protection law and its obligations by implementing data protection policies, implementing technical and organisational measures, as well as adopting techniques such as data protection by design and by default, breach notification procedures and incident response plans and ensuring all records are kept demonstrating data protection compliance.

2.3 Lawful processing

Collecting, processing and using personal data is only permitted where it satisfies one of a number of legal conditions.

One of these conditions must also be met in circumstances where the purpose for the processing of collected data changes from that for which it was originally collected.

Key conditions relevant to the Trust's operations include:

i. **Consent of the data subject**
Personal data can be processed where the data subject has provided their freely given, specific, informed and clear agreement. The data subject must be able to withdraw consent at any time. Where consent is given in writing, it must be clear and capable of being distinguished from other matters. Consent can in some cases also be given verbally.

Wherever consent is given, a record of the consent should be kept. For example, consent may be provided when a member or attendee of an event or conference completes a form or gives his/her contact details to receive communication from the Trust.

ii. **Legitimate interests**
Processing might be necessary for the purposes of the legitimate interests pursued by the Trust or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

When legitimate interest is used as a condition for processing data, a three-stage test is applied to test the balance between the Trust's interests and the rights of those who may be identified by such data. A wide range of interests may be legitimate interests. The UK GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests.

Personal data of data subjects such as authors, customers or third parties may be processed to form, execute, perform and terminate a contract.

iii. Legal obligation

According to the UK GDPR processing might be necessary for compliance with a legal obligation to which the Trust as a Controller is subject. The legal obligation must be laid down by UK law or have a sufficiently clear basis in common law.

iv. Contract

The Trust will process personal data for employment or recruitment purposes.

Processing might be also necessary for the performance of a contract. This lawful basis can be used, when the Trust needs to deliver a contractual service to an individual. For example, the Trust will enter into a contract with a data subject when for example they pay membership fees to become a member of the Trust or if they provide their bank details to make a donation to the charity.

v. Special categories of personal data

The **UK General Data Protection Regulation** identifies certain types of personal data as more sensitive and gives them additional protection. This is known as *special category data*.

Special category data includes information about a person's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (when used for identification)
- Health
- Sex life
- Sexual orientation

Under Article 9 of UK GDPR, processing special category data is prohibited unless a specific condition applies.

There are 10 permitted conditions for processing, including (but not limited to):

- Explicit consent
- Employment, social security and social protection law obligations
- Vital interests
- Legal claims
- Substantial public interest

When processing special category data, the Trust must:

1. Identify a lawful basis under Article 6 UK GDPR; and
2. Identify an additional Article 9 condition for processing.

The Data Protection Act 2018 supplements and provides further detail on these conditions.

2.4 Disclosure and Sharing of Personal Data

The Trust must take all reasonable steps to ensure that personal data is not disclosed to unauthorised Third Parties including family members, friends, government bodies and in certain circumstances, relevant law enforcement bodies.

The Trust will only share personal information in order to comply with a legal obligation, or to fulfil a contract or with a service provider who undertakes processing of personal data on behalf of the Trust under contract. The Trust may also share personal data to protect the Trust's rights, its property, or to ensure the safety of our employees. This includes exchanging information for the purposes of fraud protection or the investigation of other criminal offences.

All data collected for Disclosure & Barring Service (DBS) checks is inputted directly by the individual to the third-party external provider. No personal data relating to the DBS check is held by the Trust.

2.5 Subject Access Requests

Where a Subject Access Request is received, in any format, the Trust will make every effort to respond to such requests within once calendar month. Likewise, any other rights that a data subject may wish to exercise will be addressed within a similar time frame.

3 - RESPONSIBILITIES

3.1 Roles and Responsibilities

Data Controller: Suffolk Wildlife Trust is the Data Controller.

Governance

The Board of Trustees has overall responsibility for ensuring compliance with any applicable Data Protection Legislation. However, all employees, agents or representatives of the Trust are involved in the processing of, collection and/or controlling the contents and use of personal data are also responsible for compliance with Data Protection Legislation at an individual level.

Data Protection Lead

Name: Ellie Race
Email: ellie.race@suffolkwildlifetrust.org
Phone: 01473 924239

The Data Protection Lead is responsible for:

- Monitoring compliance
- Advising on data protection obligations
- Managing data breach responses
- Acting as contact point for data subjects and the ICO

Staff Responsibilities

All staff must:

- Process personal data in accordance with this policy
- Complete data protection training
- Report data breaches immediately
- Maintain confidentiality

Failure to comply may result in disciplinary action.

3.2 Operational oversight

The Leadership Team (SLT) is responsible for the day-to-day implementation of processes and procedures to achieve compliance with the Data Protection Legislation on behalf of the Board.

To facilitate compliance, the Trust will maintain an up-to-date Record of Processing Activities (ROPA) recording the lawful bases and declared purposes for all personal data which it processes as an organisation. This will be in conjunction with an up-to-date risk register in which any risks to the rights and freedoms of data subjects, and any related mitigation, are recorded.

The Director of Finance and Resources is the first point of contact with the Information Commissioner's Office (ICO) and also the main point of contact for data subjects where required. Their contact details will be communicated to staff and customers both on forms and on the Trust's website.

Any staff member may contact the Director of Finance and Resources in confidence whether to raise a concern, seek guidance or report an issue.

3.4 Third-Party Processors (where applicable)

In the course of its role as a Data Controller, the Trust may also engage third-party service providers, or data processors, to process personal data on its behalf.

The Trust is committed to ensuring that the use of such providers does not diminish the protections and safeguards conferred by law. In each case, The Trust will ensure that appropriate contractual arrangements are in place with the processor, setting out their obligations in relation to the personal data, the specific purposes for which they are engaged, and the understanding that they will only process the data in compliance within the data protection legislation and the UK GDPR.

In order to ensure that contractual stipulations are actually observed, where feasible, the contractual arrangements will also make clear that the Trust as Data Controller is entitled to audit or inspect the data management activities of the data processor to ensure that they remain compliant with the legislation and with the terms of the contract. It will also stipulate that in the event of a data security breach; the data processor will notify the data controller without undue delay.

4 – DATA SECURITY

4.1 IT security

All employees of the Trust are personally responsible for keeping secure any personal data controlled by the Trust and for which they are responsible. Under no circumstances may any personal data be disclosed to any third party unless the Trust has provided explicit authorisation and has entered into a confidentiality agreement, a data processor agreement, or a data sharing agreement with the third party. The Data Controller is responsible for this activity.

The Trust has IT security policies and processes which all staff are expected to be aware of and comply with these to minimise risk to our systems and data.

4.2 Location of Processing and International data transfers

The Trust processes personal data as far as is possible within the UK. Where personal data may be transferred outside the UK to a third country or an international organisation, the Trust will adopt appropriate safeguards and put in place transfer mechanisms such as the UK Addendum and the International Data Transfer Agreement as required by UK data protection law and in accordance with the guidance of the ICO.

4.3 Data Retention & Disposal

The Trust will not retain personal data for longer than is necessary. All types of data processed have been documented in the Records of Processing Activities(RoPAs) The Trust recognises the difference between certain types of data subjects for which it may be processing identifiable personal information. Personal data must be kept and deleted in accordance with the Trust's *Data retention, archiving & destruction policy***.**

5 - ENFORCEMENT AND REPORTING BREACHES

5.1 Role of the Information Commissioner's Officer (ICO)

The ICO is the National Supervisory Authority and oversees compliance with the terms of both the UK GDPR and the Data Protection Act. The ICO has a wide range of enforcement powers, including the investigation of the Trust's processing of personal data and record-keeping practices as well as the ability to levy fines, issue warnings and impose restrictions on any processing of personal data.

In all matters where the Trust has any dealings with the ICO, the Board and Leadership Team commit to full cooperation and transparency.

5.2 Incidents and breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This

includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

All staff are obliged to report any incidents regarding the incorrect or accidental processing of personal data or lost IT equipment directly to the Director of Finance and Resources without delay. This is to assist the Trust to report any breaches, where necessary, to the ICO within 72 hrs of staff becoming aware of the issue.

The Director of Finance and Resources is responsible for the assessment of incidents and the mandatory reporting of any data breaches where necessary. In their absence, all members of the Leadership Team have the authority to contact the ICO.

Affected individuals will be informed where there is a high risk to their rights and freedoms.

6 - APPROVAL AND REVIEW

Suffolk Wildlife Trust is committed to reviewing this policy and practice annually and whenever new legislation or practice makes it necessary.

Approved by SWT Board of Trustees: May 2026
Author: Operations Manager
Accountable: Director Of Finances and Resources.

Next review due: March 2027

CHANGE LOG

DATE OF CHANGE	RESPONSIBLE	SUMMARY OF CHANGE
March 2026	Operations Manager	Updated purpose and scope Added 3.1 roles and responsibilities Added reference to Data breach guidance and process
July 2024	Membership Manager Data Protection Working Group	Full policy review and formatting refresh