Sheffield & Rotherham Wildlife Trust

Data Protection Policy

Sheffield & Rotherham Wildlife Trust is committed to keeping an individual's personal details safe. We are committed to protecting the rights and privacy of individuals in accordance with the Data Protection Act (GDPR 2018) and the Privacy and Electronic Communications Regulation (PECR).

We currently **process*** data about our staff, volunteers, members, customers and other individuals involved in our work. The Trust aims to ensure that all our staff and volunteers who process this **personal data*** do so in accordance with the '6 principles of data protection', which requires that personal data:

1. **Be processed lawfully, fairly and transparently** in relation to individuals;

2. **Be collected for specific, 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 are not considered to be incompatible;

3. **Be adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;

4. **Be 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;

5. **Be time limited**; kept in a form which permits identification of an individual for no longer than is necessary for the purposes for which the personal data are processed;

6. **Be secure**; 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.

The Trust is registered as a **Data Controller*** with the Information Commissioner and as such must be able to demonstrate compliance with these principles. However, the Trust recognises that it must adhere to the principles of the Data Protection Act 2018 whether registered or not. **It is the responsibility of all Trust staff and volunteers to understand and comply with this Policy and related Procedures.**

In order to support staff and volunteers in implementing this policy, the Trust will aim to provide the following:

- Data Protection Handbook
- basic briefing to all staff and volunteers as part of their induction
- more specific data protection training and procedures for key data processing roles

*refers to 'Some Useful Definitions' – please see the end of this document.

The Trust recognises that there must be a lawful basis and purpose for processing personal data, which is determined, documented and published in our **Privacy Notices** before processing begins. There are six lawful bases for processing that the Trust can use:

1. **Consent**: the individual has given clear consent for the Trust to process their personal data for a specific purpose.
2. **Contract**: the processing is necessary for a contract between the Trust and the individual, or because they have asked the Trust to take specific steps before entering into a contract.
3. **Legal obligation**: the processing is necessary for the Trust to comply with the law (not including contractual obligations).
4. **Vital interests**: in life or death cases where an individual's medical history is disclosed to an A&E dept.
5. **Administering justice:** for exercising statutory, governmental or other public functions
6. **Legitimate interests***: the processing is necessary for the Trust's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

At least one of the above must apply whenever the Trust processes personal data and we recognise that this lawful basis can then affect which rights are available to the individual.

The Trust recognises and respects the legal rights of an individual (the 'data subject') as:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The Trust will never sell personal data.

Roles and Responsibilities

The Trust is not legally required to identify a Data Protection Officer. Key tasks will be the responsibility of the Senior Admin Officer (day-to-day) and the Exec Team, in particular, the CEO, the Head of Development and Head of Finance & Support Services.

Personal Data and Management

The Trust has compiled a **Data Audit Register**, which will be regularly updated by the Senior Admin Officer with support from the Executive Team. The register is divided in to different areas of activity across the Trust where personal data are collected. The areas include: Employees (incl payroll, pensions), Volunteers, Members, Outdoor Learning Schools, Website, Events Bookings, Marketing, Fundraising, Photo Consents, Wildscapes, IT server, Sheffield Lakeland and project participants.

For each area of Trust activity, the following information is recorded: where data is stored, what format it is in, the type of data stored eg name, address, sensitive data,

where or how the data has been collected, the use and purpose of the data, who has access to the data, access security in place, whether data can be shared and if so with whom, the process for data review and time limitations, the process for back up, removal or verification and the legal basis for holding the data (using 1-6 above).

Data Retention

The Trust aims to store personal data only for the period of time that it is required for a specific use. Details are contained in the Data Audit Register, which also acts as our Data Retention Schedule.

Risks

The most significant data breach risks to the Trust have been identified and are included in the Trust's Organisational Risk Plan, with mitigation measures put in place. The Risk Plan is reviewed by the Board every quarter.

Direct Marketing*

The Trust undertakes activities that could be considered as 'direct marketing' within GDPR & PECR. For example, through e-news 'campaign' updates or approaching members and supporters for funds. In these situations, opt-in consent will be requested. When a new, significant direct marketing activity is proposed, or we are considering relying on legitimate interests as our legal basis, the Trust will undertake a **'self-assessment and balancing'** exercise to carefully consider whether we have the appropriate legal basis for that activity and in particular whether legitimate interest, consent or a 'soft opt-in'* approach can be applied.

Reporting 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.

The Chief Executive will be responsible for reporting serious data breaches to the Charity Commission and Information Commissioner, having first notified the Chair (or Vice-Chair in their absence) and Head of Finance & Support Services, and within 72 hours for a breach likely to harm individuals involved. The Disaster Recovery Plan will also be enacted.

In the CEOs absence, the Head of Finance & Support Services, in consultation with the Chair, will report the breach to the Charity Commission and Information Commissioner.

It is the responsibility of all staff and Trustees to immediately report any personal data breach that comes to their attention to the Chief Executive or, in their absence, the Head of Finance & Support Services who, in consultation with the Chair (or in their absence the-Vice Chair), will ensure that appropriate action will be taken in accordance with this policy and related procedures.

All personal data breaches will be recorded on a breach register, irrespective of their level of risk or the need to report to the ICO.

Requests to See Data

All individuals (*data subjects*) have the right to know what personal data the Trust holds about them and can make a personal data enquiry (*subject access request*) to this effect.

Sheffield & Rotherham Wildlife Trust will aim to respond positively to any request by an individual to see the personal data we hold about them. In some exceptional circumstances, where responding to the request may require significant time and resources, the Trust may make a reasonable charge. All data requests should be made using our **Personal Data Enquiry Form.**

All requests should be directed to the Senior Admin Officer in the first instance, who will refer to the relevant senior member of staff and aim to ensure the request is responded to in accordance with this policy and within 28 days.

Disclosures

Personal data may be legitimately disclosed where one of the following conditions apply:

- The individual has given their consent (e.g. a member of staff has consented to the Trust corresponding with a named third party);
- Where the disclosure is in the legitimate interests of the institution (e.g. staff personal information can be disclosed to other Trust employees if it is clear that those members of staff require the information to enable them to perform their jobs);
- Where the Trust is legally obliged to disclose the data
- Where disclosure of data is required for the performance of a contract
- To prevent serious harm or injury

The Trust will aim to ensure we never disclose personal data to unauthorised people.

Informing People

The Trust undertakes to make every effort to ensure that when we collect personal data we are clear about how we intend to use, store and share that personal data. The Trust aims to provide **Privacy Notices** at all key data collection points eg employee recruitment, volunteer recruitment, membership recruitment, website landing & forms. These can also be found on our website.

The personal data the Trust collects may also include the less traditional collection methods categories identified by the ICO eg social media location data for targeted adverts.

Review

We will review this Policy regularly and at least annually.
Next review date: May 2019.

Related Trust Policies and Procedures:

Data Protection Policy & Procedure Handbook

HR Handbook (Recruitment etc)

Safeguarding Children, Young People & Vulnerable Adults

Fundraising Policy and Procedures

Finance and Investment Policy and Procedures

Events and Activity Bookings

*refers to 'Some Useful Definitions' – please see the end of this document.

*Some Useful Definitions (ICO website)

Data Processing

This refers to any operation performed on personal data (or data sets), that is manual, automated or otherwise, which collects, records, organises, structures, stores, adapts, alters, retrieves, consults, uses, discloses, transmits, disseminates or otherwise makes available, aligns or combines, restricts, erases or destroys.

Personal Data

GDPR covers Personal Data and Sensitive Personal Data (now to be known as Special Categories of Personal Data – see below).

For data to be classified under Personal Data it must:

1. Be data (so not unrecorded conversations with service users, donors or customers); and

2. Be personal. Data is personal if it is concerned with identifiable, living individuals. It does not matter whether this data was processed automatically, electronically or manually.

Some more unusual examples:

Someone participating in an online forum, only known to the Trust by their username. The information we hold, relating to their posts and other activity, would be personal data.

A photograph where someone is clearly distinguishable, even if the Trust does not know their name, is personal data.

Personal data has been expanded to include IP addresses, internet cookies and biometrics, such as, DNA and fingerprints. It is common for IP addresses to be collected by websites or marketing campaign websites such as Mailchimp – and so this personal data needs to be secure.

Special categories of personal data contain information about:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- health
- sex life or sexual orientation
- genetic data
- biometric data where processed to uniquely identify an individual

An organisation is a **Data Controller** if it "*determines the purposes and means of the processing of personal data".*

Legitimate Interests

'*Legitimate interests*' is different to the other lawful bases as it is not centred around a particular purpose (eg performing a contract with the individual, complying with a legal obligation, protecting vital interests or carrying out a public task), and it is not processing that the individual has specifically agreed to (consent). Legitimate

interests is more flexible and could in principle apply to any type of processing for any reasonable purpose.
Because it could apply in a wide range of circumstances, it puts the onus on us to balance your legitimate interests and the necessity of processing the personal data against the interests, rights and freedoms of the individual taking into account the particular circumstances.
The ICO proposes three tests in the following order to help organisations assess their use of 'legitimate interest':

- **Purpose test** – is there a legitimate interest behind the processing? eg. processing membership and supporters data and direct marketing to our contacts in order to improve grow our membership and promote our charitable objects.
- **Necessity test** – is the processing necessary for that purpose?
- **Balancing test** – is the legitimate interest overridden by the individual's interests, rights or freedoms?

You must be able to satisfy all three parts of the test prior to commencing your processing.

Direct Marketing

For the purposes of GDPR, direct marketing is defined as:

"the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals" (ICO Guidance Direct Marketing May 2018).

The guidance goes on further to consider direct marketing in a not-for-profit context:
"Direct marketing is not limited to advertising goods or services for sale. It also includes promoting an organisation's aims and ideals. This means that the direct marketing rules in the DPA and PECR will apply to the promotional, campaigning and fundraising activities of not-for-profit organisations. For example, a charity or political party contacting particular individuals to appeal for funds or votes, or contacting supporters to encourage them to write to their MP or attend a public meeting etc….."

Soft Opt-In

This can be applied to existing customers**.**
This means organisations can send marketing texts or emails if:

- they have obtained the contact details in the course of a sale (or negotiations for a sale) of a product or service to that person;
- they are only marketing their own similar products or services; **and**
- they gave the person a simple opportunity to refuse or opt out of the marketing, both when first collecting the details and in every message after that.

Charities, political parties or other not for-profit bodies will not be able to rely on the soft opt-in when sending campaigning texts or emails, even to existing supporters. In other words, texts or emails promoting the aims or ideals of an organisation can only be sent with specific consent.

NB the Trust mainly promotes its work using the e-newsletter, which people are asked to sign up for if they wish to receive it ie they have to give their consent/opt-in to receive it.

*refers to 'Some Useful Definitions' – please see the end of this document.