Data Protection Policy and Procedure for Bird Song Trust (the "Trust)

Approved March 2025

1. Introduction

The Data Protection Policy and Procedure sets out the framework for handling, storing and deleting data, including personal data at Bird Song Trust.

Bird Song Trust is committed to responsible use of data in relation to all our stakeholders' information, and to compliance with the General Data Protection Regulations (GDPR).

2. Scope

This policy applies to Trustees, staff and volunteers of the Trust.

3. Responsibility

The Trustees have overall responsibility for the operation of this Policy and Procedure, for determining the administrative processes to be followed, and the format of the records to be kept.

4. GDPR

GDPR applies to all 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified from that data. GDPR applies to automated personal data and manual filing systems.

Under the GDPR, the data protection principles set out the main responsibilities we must follow at the Trust. Personal data shall be:

• Processed lawfully, fairly and in a transparent manner in relation to individuals

• Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes

• Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

• Accurate and, where necessary, kept up to date

• 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

• 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

To ensure we comply with these principles, we are committed to protecting individual rights. Please see Appendix 1 for full details about subject access rights.

If any data breaches occur, we have a clear policy and process for reporting, as highlighted in Appendix 2. All staff receive information and training about reporting data breaches and we encourage a culture of reporting.

5. Commitments

To ensure data protection is carried out diligently across the organisation the Trust has committed to:

• Providing data protection training to all staff and volunteers and refreshed every 3 years.

• Maintaining agreements with all data processors we are working with detailing their commitment to comply with GDPR regulations.

• Carrying out a data protection impact assessment when dealing with new types of data. These will be reviewed as necessary to ensure they are accurate and sufficient.

• Having a clear and robust procedure for reporting data breaches (see Appendix 2). All data held by the Trust is identified as to its sources, where it is held, who has access, the lawful basis for holding and processing it and the period of time it should be held for.

Where the basis for holding information is consent, this consent is obtained clearly to ensure the data subject fully understands what data the Trust will be holding and how it will be used.

This policy should be read in conjunction with other policies that relate to processing and retaining information.

For further information, detail and guidance please refer to the Information Commissioners Office (ICO) https://ico.org.uk

Appendix 1: Subject Access Rights (SARs)

All individuals for whom we hold or process data have the following rights. For further details on the rights below please refer to the Information Commissioners Office (ICO) https://ico.org.uk

Right to be informed

Data subjects can contact the Trust as the data controller and request information on what data is held and processed.

Right of access

Access to personal data may be requested to verify and ensure data processing is lawful. Data must be provided to the data subject within one month of the request or two months by extension if the request is complex. Data must be provided free of charge unless the requests are unfounded or repetitive. The identity of the subject must be confirmed before any response is made.

Data can be provided in paper form or secure electronic means (e.g. encrypted email).

Right to rectification

If data held is inaccurate or incomplete, a data subject can ask for it to be rectified. This must be done and a response sent within one month of the request (or two months by extension if the request is complex). If we do not feel data can or should be rectified, we need to inform the data subject of this and provide details about their right to complain to ICO.

Right to erasure (right to be forgotten)

A data subject has the right to request that their data is permanently deleted. There is only an obligation to destroy data if it was obtained as a result of consent which has now been withdrawn or the data is no longer needed for the original purpose for which it was obtained.

If there is a legal reason to keep the data, the right of erasure can be refused.

Erasure does not need to apply to all data, data that is unreasonably difficult to access such as that kept in a remote archive will not necessarily need to be erased.

The data subject must be informed when the data is erased or the reason their right to erasure has been refused.

If data has been shared with third parties, they must be informed of the erasure request.

Right to restrict processing

In the interim period where a right to erasure is being considered the data processor or controller will only be able to store limited data and will not be able to process it.

Right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows an individual to move, copy or transfer data easily from one IT environment to another in a safe and secure way without hindrance to usability. This only applies where consent was given to collect and process data initially and the process is done by an automated means.

Requests must be completed within a month and we must respond to the individual if we are not able to comply, making them aware of their right to complain.

Right to object

Individuals have the right to object if they feel their data is being processed or stored inappropriately. This right is absolute, and all processing of this data must be stopped if it is being used for marketing purposes. Where other bases are used to obtain, hold and process information the subject must demonstrate grounds relating to his or her particular situation.

Rights regarding automated decision making and profiling

Automated decision making and profiling is allowed only when it is necessary and must be based on an individual's explicit consent. It is prohibited if it can adversely affect someone's legal rights.

Appendix 2: Personal Data Breaches

To comply with GDPR and to safeguard personal information the Trust will report personal data breaches without delay (within 72 hours of the breach being identified). The purpose of data breach reporting is to mitigate potential losses to the organisation and any individuals affected and to improve systems and training.

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

All breaches will be examined to identify further actions which could include:

• Reporting to Information Commissioners Office (if the breach is likely to risk an individual's rights and freedoms)

• Make the individuals whose data has been breached aware

• Providing further training and guidance to prevent re-occurrence

Any breach of confidentiality and personal data should be reported to the Director, who will then appoint an appropriate independent person (e.g. a member of the board of trustees or a senior member of staff) to investigate the matter. If, following a written summary of findings, the Director finds that a breach has occurred, they have the discretion to take appropriate action within 28 days. This may include consideration of pursuing disciplinary action or, in the case of a volunteer, asking the person to withdraw from Bird Song Trust's service.

Appendix 3: Guidance to staff

Different kinds of data may be kept by Bird Song Trust, such as recruitment and selection data, employment records, sickness records, pension or insurance scheme records, disclosure, etcetera. Information used for any of these purposes must be used for those express purposes only and must be kept securely.

Staff have a legal right of access to the information Bird Song Trust holds on them and the right to challenge the information if it is thought to be inaccurate or misleading. If a staff member objects to Bird Song Trust holding or using information about them because it causes them distress or harm, Bird Song Trust will delete the information or stop using it in the way complained about unless Bird Song Trust has a compelling reason to continue holding and/or using that information.

Bird Song Trust's employees should bear in mind the following considerations:

- Sensitive and confidential information must be treated with particular attention.
- Personal data must not be emailed to staff members' personal email accounts, as there is no guarantee of security of these accounts.
- Any personal data should not be stored in paper format without express permission from the Director, in which case the Director will advise how to store confidential information.
- All Bird Song Trust computers must be password protected. All personal data should be kept in the appropriate IT system. If electronic equipment is lost or stolen, access to the server and database from that piece of equipment will be severed.
- The database holding customers' personal data must be accessed only via Bird Song Trust's electronic equipment. All employees and volunteers will be trained on how to use the database relying on the written procedures for entering, amending and maintaining data.
- Any changes to personal data (e.g. a change in home address) must be updated within 28 days of receipt.
- Personal data must not be given out to any third party unless the individual has agreed to release this information.
- Any personal data kept in paper format that is no longer required must be destroyed.
- Any personal data kept electronically that is no longer required must be deleted. Bird Song Trust will carry out data minimisation as part of the annual data audit.