

2025



# Data Protection Policy

**FINDHORN NAIRN AND LOSSIE  
RIVERS TRUST**

## CONTENTS

1. Introduction	2
2. Lawful, Fair, Transparent	2
3. Purpose Limitation	3
4. Data Minimisation	3
5. Accuracy	3
6. Storage Limitation	3
7. Integrity and Confidentiality (Security)	3
8. Rights of Individuals	4
9. Data Breaches	4
10. Policy Review	5

## I. Introduction

- 1.1. The Findhorn Nairn & Lossie Rivers Trust (FNLRT) is a registered charity (number: SC040152) and Company Limited by Guarantee (Company number: 350687) and is Data Controller with the Information Commissioners Office (ICO) (Registration: ZA094408).
- 1.2. In the course pursuant to its charitable objects, it may be necessary for FNLRT to process personal data. This policy provides guidance to staff on compliance with data handling regulations and transparency to beneficiaries and stakeholders whose data it may need to process.
- 1.3. This policy applies to all personal data processed by FNLRT; personal data is defined as any information relating to an identified or identifiable living individual.
- 1.4. FNLRT accepts that it is a data controller for the purposes of the General Data Protection Regulation (GDPR) and that it must comply with the following five principles for the handling of personal data:
  - *Lawful, Fair, and transparently processed* – when FNLRT needs to process personal data, it will do this in line with current legislation and be clear on why it needs the data and open and honest about how it will handle it.
  - *Purpose limitation and data minimisation* – FNLRT will limit the data collected to only what it requires for the purpose stated and will not use personal data for purposes out with this. FNLRT will ensure that the purpose is legitimate and will not further process personal data in a manner that is incompatible with the original purpose.
  - *Accurate* – data will be kept up to date and reasonable steps taken to ensure that any inaccurate data is amended or removed as appropriate.
  - *Storage limitation, integrity and confidentiality* – data collected and stored will not be kept in a way that people can be identified from it longer than is necessary.
  - *Processed in a way that ensures appropriate security* – data will be protected against accidental or unauthorised access, destruction, loss, use, modification, or disclosure
- 1.5. The FNLRT Administrator is responsible for the day to day implementation of the policy and is the Data Protection Officer (DPO) for FNLRT. All employees have a responsibility to familiarise themselves with the Data Protection Policy and to ensure that any data processed in the course of employment role adheres to data protection regulations.

## 2. Lawful, Fair and Transparent

- 2.1. To ensure its processing of personal data is lawful, fair and transparent FNLRT will:
  - Maintain an accurate and up to date Data Controller database which records where and why we process personal data. These records will also include detail on the lawful basis for having this personal information which must fall under one of the following:
    - consent
    - contract,
    - legal obligation,
    - vital interests,
    - public task
    - legitimate interests
  - Ensure compliance with the Data Protection Policy to prevent personal data from being used unlawfully.
  - The Data Controller database will be reviewed at least annually.
- 2.2. The way that FNLRT collects and processes personal data through its website is detailed in the Privacy Notice which is also available on the website. This notice is reviewed annually.
- 2.3. When collecting personal data for any reason, FNLRT will be honest and open about what it will use this information for and will not use it for any other purposes.

- 2.4. FNLRT acknowledge individuals' rights to access their personal data and any requests for this information will be dealt with within 28 days of receipt of a request.

### 3. Purpose Limitation

- 3.1. When considering collecting personal data a clearly defined purposes must be outlined and communicated clearly. This must be recorded in the Data Controller database.
- 3.2. Where the purpose is detailed in the Privacy Notice, this will be reviewed at least annually or when a change is identified.
- 3.3. Personal data collected for a specific purpose can only be used for a new purpose if it is compatible with the original purpose. If it is not compatible, written consent must be obtained before this data can be used.

### 4. Data Minimisation

- 4.1. FNLRT will develop data collection processes that only collect the personal data that is actually needed to fulfil the purpose, is adequate and relevant.
- 4.2. Data collected will be reviewed annually and any information no longer needed will be deleted or destroyed.

### 5. Accuracy

- 5.1. FNLRT will take all reasonable steps to ensure that the personal data it holds is accurate.
- 5.2. If the purpose of processing personal data requires that it is updated FNLRT will undergo a process of confirming the accuracy of the data. If it is discovered that personal data held is incorrect or misleading, reasonable steps will be taken to correct or erase it as soon as practicably possible.

### 6. Storage Limitation

- 6.1. FNLRT will not keep personal data for longer than it needs to for the purpose the data was collected.
- 6.2. The purpose of collecting the data will inform how long it is kept. FNLRT has a Document Retention Policy which identifies areas where personal data is processed, how long it will be kept, justification for why it is needed and how it will be removed.
- 6.3. Personal data may be kept for longer for public interest archiving, scientific or historical research or for statistical purposes, in this case, this will be clearly identified.
- 6.4. Data held will be annually audited in line with the Data Protection Policy and Document Retention Policy.
- 6.5. FNLRT acknowledges an individual's 'right to be forgotten' and agrees to erase any personal data held on request.

### 7. Integrity and Confidentiality (Security)

- 7.1. FNLRT will hold all personal data securely. Digital data will be stored using secure software that is kept up to date and appropriately backed up to a secure location.
- 7.2. When data is deleted or destroyed, hard copies will be shredded, and digital copies will be irrecoverably deleted.
- 7.3. Access to personal data will be restricted to authorised personnel as deemed appropriate to the purpose of data control
- 7.4. The DPO will provide a point of contact to advise on implementing the Data Protection Policy and will coordinate training for employees on cybersecurity and data protection/GDPR.

## 8. Rights of individuals

- 8.1. Individuals have the right to access their personal data and any such requests made to FNLRT shall be dealt with in line with legal requirements, with some limited exceptions.
- 8.2. The UK GDPR provides the following rights for individuals in relation to their personal data:
- the right to be informed – FNLRT does this by making sure its privacy notices are correct and up to date and direct individuals to these notices on the FNLRT website
  - the right to access their own data – any subject access requests must be notified to the FNLRT Data Protection Officer (DPO) who will co-ordinate a full search all FNLRT's systems before responding to the individual within 28 days, as required by law.
  - rectification – FNLRT will quickly update any personal data which has been identified as inaccurate or incorrect.
  - erasure – FNLRT will remove any personal data if an individual request this, unless it has another lawful basis which would prevent this e.g. employee records cannot be deleted as FNLRT is required to keep these to comply with other legislation
  - to restrict processing - where there is a dispute about the accuracy, validity or legality of personal data held by FNLRT, an individual has the right to require FNLRT ceases processing the data for a reasonable period of time to allow the dispute to be resolved.
  - the right to data portability - FNLRT will provide an individual with their data in a common and machine-readable electronic format.
  - the right to object – complaints or objections to processing personal data will be dealt with quickly and accurately.
  - rights in relation to automated decision making and profiling – FNLRT does not carry out any automated decision making or profiling of any individual.

## 9. Data Breaches

- 9.1. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, FNLRT shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the Information Commissioner's Office (ICO).
- 9.2. All trustees, staff and volunteers must be able to identify a suspected personal data breach. A breach could include:
- access by an unauthorised third party to personal data;
  - deliberate or accidental action (or inaction);
  - sending personal data to an incorrect recipient;
  - computing devices containing personal data being lost or stolen;
  - alteration of personal data without permission; and
  - loss of availability of personal data.
  - leaving a file on a train.
- 9.3. Where a member of staff discovers or suspects a personal data breach, this should be reported to the DPO as soon as possible. Where there is a likely risk to individuals' rights and freedoms, the DPO will report the personal data breach to the ICO within 72 hours of FNLRT being aware of the breach. Where there is also a likely high risk to individuals' rights and freedoms, we will inform those individuals without undue delay.
- 9.4. The DPO will keep a record of all personal data breaches reported and follow up with appropriate measures and improvements to reduce the risk of reoccurrence.

## 10. Policy Review

10.1. The Data Protection Policy will be reviewed by the Board of Trustees annually or when required by process changes or legislation requirements.