Data Protection and ICT Policy

Document Control Sheet

Key Information

Title:	Data Protection and ICT Policy
Prepared By:	Lesley Spuhler, CEO
Authorised By:	Finance, Audit and Risk Committee
Original:	Feb 2023
Approved By:	Trustees
Date of Commencement:	Feb 2023
Review Frequency:	Every 2 Years
Date of Last Review:	March 2025
Date of Next Review:	March 2027

Key Changes

Date	Summary of Changes	Section Number	Initials
Feb 23	New policy		LS
June 24	Quality Check complete document		DH
Feb 25	Approved by FAR Committee		LS
March 25	Ratified by Trustees		LS
19/05/25	New control sheet added and updated. Amended document header.		DH

Contents

1. Policy Statement

The Foundation of Light (FOL) handles personal data in a way which protects the interests and confidentiality of its participants, staff, volunteers, and other stakeholders. The FOL's management systems and processes operate in compliance with applicable legal obligations and good practice guidelines. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default. The FOL also takes its accountability for IT and cyber security seriously to protect the confidentiality, integrity and availability of FOL information.

The purpose of the Data Protection and ICT Policy is to support the seven GDPR Principles, the General Data Protection Regulation (2016), the Data Protection Act (2018), the common law duty of confidentiality, computer misuse (1990), the Copyright Act (1988), health and safety legislation and all other relevant national legislation.

The FOL is Information Commissioner's Office registered.

2. Policy Aim

As the reliance on Information Technology for any modern business increases, it makes it necessary to ensure that systems are developed, operated, used, and maintained in a safe and secure manner, reducing risk whilst also aiding effectiveness and productivity.

As the requirement for data transmission increases, we become more vulnerable to accidental or deliberate security breaches.

This policy aims to ensure that employees of the FOL understand the way in which Information Technology (IT) hardware and software including, but not limited to, electronic mail (e-mail) and the Internet should be used in the organisation.

It intends to ensure that all staff are aware of their responsibility and that breach of this policy may result in civil or criminal liability and/or breach of contract of employment with the Foundation that may lead to disciplinary action and termination of employment.

3. Scope

The policy (and accompanying manual) applies to all employees, Board Members, partners, and volunteers of the Foundation. It also applies to contractors and visitors, not employed by the Foundation but engaged to work with or who have access to Foundation information, for example, computer maintenance contractors, Foundation partners, and consultants working on behalf of the Foundation.

Participants use of ICT procedures including ESafety are detailed in the Quality Manual.

4. Definitions

Information - covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created.

General Data Protection Regulation (GDPR): the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

Seven Principles of GDPR: accountability, integrity and confidentiality, storage, limitation, accuracy, data minimisation, purpose limitation, lawfulness, fairness and transparency.

Consent: freely give, specific, informed and unambiguous agreement by the Data Subject to the Processing of their Personal Data. Consent must be made by a clear positive action and cannot be implied.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own purposes.

Data Retention: the schedule attached to this Policy containing the retention periods relating to Personal Data Processed by the Foundation.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify from that data alone or in combination with other information we possess or can reasonably access. Personal Data includes Sensitive Personal Data. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security or confidentiality of Personal Data or the physical or technical safeguards that we or our third-party service providers put in place to protect such Personal Data. The loss, unauthorised access or disclosure of Personal Data is a Personal Data Breach.

Privacy Notices (also referred to as Fair Processing Notices): separate notices setting out information that may be provided to Data Subjects when the Foundation collects information about them.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

5. Policy Principles

Leadership, Governance and Culture

Data Protection and ICT safety is everyone's responsibility. The FOL has a designated Data Protection and ICT Lead reporting to the Assistant Director – Compliance, who has access to the Board and professional advice when required. There is a Data Controller.

Roles, Responsibilities and Training

The Data Protection and ICT Lead is responsible for overseeing Data Protection, GDPR and ICT safety across the company including informing the ICO of any losses of personal data. Day-to-day activities are managed through a scorecard. Users are responsible for notifying the Lead in any suspected breach of ICT security.

All employees undertake annual training.

General GDPR Principles
We will establish and maintain policies to ensure compliance with the Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the General Data Protection Regulation and all other relevant legislation.

We will establish and maintain procedures for the controlled and appropriate sharing of service user and staff information with other agencies, taking account all relevant legislation and citizen consent.

Where consent is required for the processing of personal data, we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time through processes which have been explained to them and which are outlined in our Record Keeping Procedure. We ensure that it is as easy to withdraw as to give consent.

We will undertake annual audits of our compliance with legal requirements.

We acknowledge our accountability in ensuring that personal data shall be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- Accurate and 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 ('storage limitation');
- Processed in a manner that ensures appropriate security of the personal data.

We uphold the personal data rights outlined in the GDPR;

- 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

Procedures and Practices
The FOL has a Data Protection and ICT Manual with relevant procedures. The procedures cover cyber security; data retention; data breach; privacy, clear desk, fair processing, destruction and sensitive data. It defines processes for storing, access, subject access

requests and consent. It also covers acceptable use; confidential data; network access; emails; passwords; social media; physical security; and working with at risk participants.

There is an annual audit and Data Mapping exercise that collects what, where, why, how, when, and who of the Data. The policy is scrutinised by the Finance, Audit and Risk Committee.

It links with other policies and manuals including health and safety, quality and people.

Educating and Empowering
The FOL's induction process for staff, volunteers and Trustees includes data protection training. This training is provided immediately, if the position involves direct data contact, and in other cases, within one month of joining the FOL.

There is ongoing training for all staff, volunteers, and Trustees, which includes bi-annual refreshers through the FOL's Equal system; updates on changes to the policy and procedures; and after incident reviews to learn from incidents and near-misses.

The FOL maintains up-to-date records of inductions and ongoing training including dates, attendance and the matters covered on the PeopleHR system.

Managing Incidents
Concerns and complaints are taken seriously and investigated swiftly. The FOL acts as necessary, including reporting incidents to the relevant authority where appropriate.

The FOL's policy and procedures make specific provision for the management of data protection breaches, including communication with stakeholders, including where relevant the Charity Commission and consequences for breaches, including disciplinary procedures and dismissals.

Equality, Diversity and Inclusion
We will ensure that equality is embedded in all our activities, policies and decisions and will work with our partners to share good practice.

5. Policy Ratification and Review

This Policy was reviewed and approved by the Board of Trustees on 14 February 2023. The Policy will be reviewed every two years.