DATA PROTECTION POLICY

1. POLICY OUTLINE

This policy sets out the obligations and expectations on employees of FLH including contractors, temporary staff and any volunteers or Trustees with regards to any and all information used or input onto any computer or media device (including the charity's hardware or home devices).

Future Living Hertford (FLH) is fully committed to compliance with the requirements of the Data Protection Act 2018 which updates the Data Protection Act 1998. A component of the 2018 Act and General Data Protection Regulation (GDPR) requirements is to ensure that personal data is stored securely.

1.1 Dissemination

This Policy and Procedure will be made available for all staff, Trustees, and volunteers to read during their Induction process.

All Trustees and any staff who are working in any capacity for the charity are required to understand and commit to the working practices outlined in the Policy and Procedures.

2. SCOPE AND DEFINITIONS

This policy applies to all employees, volunteers and Trustees of FLH, regardless of whether they have access to the charity's computer systems. It pertains to all digital information used or input by the charity, including that related to clients, services, colleagues and third parties.

3. PRINCIPLES

- All FLH computers will be password protected
- No person is allowed to use FLH IT facilities without authorisation by a line manager or the C.E.O.
- All email correspondence entered into on behalf of the charity should be conducted only through an FLH email account. (The exceptions to this rule are Trustees of the charity who may correspond through personal or business accounts).
- The charity's computer systems will be protected by appropriate security software (e.g. firewalls).

4. RESPONSIBILITIES

The C.E.O. and Board of Trustees are responsible for ensuring that the Data Protection practices within the charity are maintained and that any breaches or lapses are identified, controlled and rectified. Should any serious security or malicious breaches occur, these should be reported to the Trustees as soon as is practicable by the C.E.O.

A serious breach is one in which security of the IT system is compromised, or where sensitive or confidential information is liable to be, or has been, accessed by those not authorised to do so, or where a threat to the security of the charity's data has been identified (e.g. by hacking/breach of a firewall).

5. COMPLIANCE

It is the responsibility of Future Living Hertford's Trustees and the C.E.O. to ensure compliance and the effectiveness of the procedures accompanying this policy.

Breaches in the procedure will be treated as serious offences and should be reported in the first instance to the C.E.O. who will then report them to the Trustees at the next Board meeting or, if serious breaches occur which have legal consequences, the C.E.O. is duty-bound to report them to the Board of Trustees immediately.

Should the C.E.O. be found to be in non-compliance to UK legislation or guidance then the matter will be treated as a disciplinary matter.

6. RELATED POLICIES AND PROCEDURES

Disciplinary Policy and Procedures
Complaints Policy and Procedures
Grievance Policy and Procedures
Whistleblowing Policy and Procedures
Internet and Email Usage Policy and Procedures
Safeguarding Policy and Procedures
Confidentiality Policy and Procedures
External Communications Policy and Procedures
Internal Communications Policy and Procedures
Induction Policy

7. LEGAL FRAMEWORK

The Data Protection Act 2018
Freedom of Information Act 2000
Computer Misuse Act 1990
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
The Charities Act 2011

DATA PROTECTION PROCEDURE

1. CONTEXT

In order to operate efficiently, Future Living Hertford ("FLH") has to collect and use information about people with whom it works. These may include client (current, past and prospective), staff, volunteers, suppliers and other third parties. In addition FLH may have a requirement by law to collect and use information in order to comply with the requirements of central government.

This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

Given the nature of the service and its aims and principles, FLH views the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between FLH and those with whom they carry out business.

To this end, Future Living Hertford fully endorses and adheres to the principles of data protection as set out in the Data Protection Act 2018.

2. APPLICATION

2.1 The Principles of Data Protection

FLH is committed to processing data in accordance with its responsibilities under the Data Protection Act 2018.

Article 5 of the GDPR requires that personal data shall be:

a) Processed fairly and lawfully and in a transparent manner in relation to individuals;
b) Collected for specified, 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 shall not be considered to be incompatible with the initial purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data

may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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 Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and 'sensitive' personal data.

Personal data is defined as data relating to a living individual who can be identified from:

- that data
- that data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

Sensitive personal data is defined as personal data consisting of information as to:

- racial or ethnic origin
- political opinion
- religious or other beliefs
- trade union membership
- physical or mental health or condition
- sexual life
- criminal proceedings or convictions

In 2018 the Act was updated to make data protection laws fit for the digital age.

The Act introduced stronger sanctions for malpractice as well as standards for protecting general data through the General Data Protection Regulation (GDPR) which is a regulation in EU law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The Regulation aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. It allows individuals more control over the use of their data and provides them with rights to move or delete their personal data.

Any information which the charity holds is potentially disclosable to a requester under the Data Protection Act 2018 or the Freedom of Information Act 2000. This includes emails.

Users need to be sure that they are not breaching any data protection when they write and send emails. This could include, but is not limited to:

- Passing on personal information about an individual or third party without their consent;
- Keeping personal information longer than necessary;
- Sending personal information to a country outside the EEA.

Email should, where possible, be avoided when transmitting personal data about a third party. Any email containing personal information about an individual may be liable to disclosure to that individual under the Data Protection Act 1998. This includes comment and opinion as well as factual information.

2.2 Handling of personal/sensitive information

FLH will, through appropriate management and the use of strict criteria and controls:

- Observe fully conditions regarding the fair collection and use of personal information
- Meet its legal obligations to specify the purpose for which information is used
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Apply checks to determine the length of time information is held
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information is not transferred abroad without suitable safeguards
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act

These include:

- The right to be informed that processing is being undertaken
- The right of access to one's personal information within the statutory 40 days
- The right to prevent processing in certain circumstances
- The right to correct, rectify, block or erase information regarded as wrong information

In addition, FLH will ensure that:

- There is someone with specific responsibility for data protection in FLH
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice
- Everyone managing and handling personal information is appropriately trained to do so
- Everyone managing and handling personal information is appropriately supervised
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or volunteer or a member of the public, knows what to do
- Queries about handling personal information are promptly and courteously dealt with
- Methods of handling personal information are regularly assessed and evaluated
- Performance with handling personal information is regularly assessed and evaluated
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All staff and volunteers are to be made fully aware of this policy and of their duties and responsibilities, and will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. In particular they will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment
- Personal data held on computers and computer systems is protected by the use of secure passwords
- Individual passwords are such that they are not easily compromised

2.3 Implementation

- This policy applies to all personal data processed by FLH.

- The Chief Executive Officer (C.E.O.) shall take responsibility for FLH's ongoing compliance with this policy.

- This policy shall be reviewed at least annually.

- FLH shall register with the Information Commissioner's Office as an organisation that processes personal data.

2.4 Notification to the Information Commissioner

The Information Commissioner is an independent official whose role is to uphold information rights in the public interest, promoting openness by publish bodies and data privacy for individuals. The Commissioner investigates complaints as well as conducting proactive investigations. As well as being an enforcer, the Commissioner acts to inform and educate data controllers, and the wider public, to improve standards.

The Information Commissioner maintains a public register of data controllers. FLH will be registered as such.

The Data Protection Act 1998 requires every data controller who is processing personal data to notify and renew their notification on an annual basis. Failure to do so is a criminal offence. The 2018 Act makes provision to allow the Commissioner to continue to operate under the new data protection laws.

The 2018 Act requires data controllers for both general data and law enforcement purposes to notify the Commissioner within 72 hours of a data breach taking place, if the breach risks the rights and freedoms of an individual. In cases where there is a high risk, businesses must notify the individuals affected.

The C.E.O. will review the Data Protection Register annually in December, prior to notification to the Information Commissioner.

Any changes to the register must be notified to the Information Commissioner within 28 days. To this end, any changes made between reviews will be brought to the attention of the Director of Corporate Affairs immediately.

2.5 Lawful, fair and transparent processing

a) To ensure its processing of data is lawful, fair and transparent, FLH shall maintain a Register of Systems.
b) The Register of Systems shall be reviewed at least annually.

c) Individuals have the right to access their personal data and any such requests made to FLH shall be dealt with in a timely manner.

2.6 Requests for information

All requests to view, move or delete data that the charity holds should be directed to the C.E.O. in the first instance.

2.7 Lawful Purposes

a) All data processed by FLH must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
b) FLH shall note the appropriate lawful basis in the Register of Systems.
c) Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d) Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in FLH's systems.

2.8 Data minimisation

FLH shall ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

2.9 Accuracy

a) FLH shall take reasonable steps to ensure personal data is accurate.
b) Where necessary for the lawful basis on which data is processed, steps shall be put into place to ensure that personal data is kept up to date.
c) FLH utilises the Lamplight data entry system.

2.10 Archiving/removal

a) To ensure that personal data is kept for no longer than necessary, FLH shall put into place an archiving policy for each area in which personal data is processed and review this process annually.
b) The archiving policy shall consider what data should/must be retained, for how long, and why.

2.11 Security

a) FLH shall ensure that personal data is stored securely using modern software that is kept up-to-date.
b) Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c) When personal data is deleted this should be done safely such that the data is irrecoverable.
d) Appropriate back-up and disaster recovery solutions shall be in place.

2.12 Breach

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, the Charity shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

3. REVIEW AND COMPLIANCE

This Policy and Procedure will be reviewed annually by the C.E.O. or a delegated member of staff. Where revisions are required these must be ratified by a quorate of the Trustees.

To ensure compliance to this Policy, one Trustee will be elected to oversee the planning process and ensure that all planning is in line with this policy. The Trustee currently elected to ensure compliance in this area is Charles Fraser.