Forest of Hearts Data Protection and GDPR Policy

Introduction

Forest of Hearts needs to gather and use certain information about individuals to fulfil its purpose(s) and acts as a Data Controller as defined by legislation.

This policy describes how this personal data will be collected, handled and stored to meet the Organisation's data protection standards and to comply with legal requirements.

This data protection policy ensures Forest of Hearts:

- Complies with data protection law and follows good practice
- Protects the rights of staff, volunteers, service users and other stakeholders
- Provides clarity about how it stores and processes personal data
- Protects against the risks of a data breach.

This policy applies to all activities conducted by Forest of Hearts and all persons working on its behalf involving any and all data relating to identifiable individuals.

Data Protection Law

This policy is based upon the UK Data Protection Act 1998 and the General Data Protection Regulation (GDPR) which operates within EU Regulation 2016/679. These provide a robust model for Data Protection and Privacy compliance and apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal data must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act was underpinned by eight important principles. These say that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be secured and protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Article 5 of the GDPR clarified these requirements by stipulating that 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 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;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

Forest of Hearts Data Protection and GDPR Policy

- 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;
- 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; (although 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
- 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.

Definitions

The following definitions apply within this document:

Breach	The unlawful disclosure, loss or destruction of personal data being processed.
Consent	Freely given, unambiguous statement indicating a data subject's wishes agreeing to the processing of specified personal data relating to himself or herself.
Data Controller	An organisation or person determining the purposes and means of processing personal data
Data Owner	The person to whom the management of purposes and means of processing personal data may be delegated by the data processing officer.
Data Processing Officer	The person appointed by a data controlling organisation to determine the purposes and means of processing personal data
Data Processor	Personal or third party agent processing data on behalf of a data controller.
Data Protection	The process of safeguarding personal data from unauthorised or unlawful disclosure, access, alteration, processing, transfer or destruction.
Data Subject	The identified or identifiable living person to which personal data refers.
Personal Data	

Forest of Hearts Data Protection and GDPR Policy

	Any information relating to a living person from which they can be directly or indirectly identified.
Processing	Collection, recording, storage, retrieval, alteration, copying, consultation, transmission, dissemination, archiving or deletion of personal data in any form.

Data Subject GDPR Rights

Every Data Subject has Data Protection Rights under the Regulations. There include:

The right to be informed

Forest of Hearts must provide Data Subjects with various pieces of information about the data processing activities carried out with their personal data, in a concise, transparent, intelligible and easily accessible manner and without charge.

The right of access

Forest of Hearts must provide Data Subjects with confirmation their data is being processed and access to their personal data within one month of receipt of a request for such access. This must be without charge unless the request is 'manifestly unfounded or excessive'.

The right to rectification

Forest of Hearts must provide Data Subjects with rectification of their personal data if it is inaccurate or incomplete, within one month of receipt of such a request.

The right to be forgotten

Forest of Hearts must provide Data Subjects with the right to withdraw consent for their data to be processed and to be removed from records.

The right to object

Forest of Hearts must provide Data Subjects with the right to object, or challenge, the use of their personal data if held under grounds other than their consent. In such cases the use of that data must be ceased unless processing the personal data unless compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual, can be demonstrated or the processing is for the establishment, exercise or defence of legal claims.

The right to restrict processing

Forest of Hearts must provide Data Subjects with the right to restrict processing in certain defined circumstance including the suspension of processing whilst requests for other rights are being processed or the delay of disposing records beyond their retention period because of a Data Subject's need for them to be retained.

Forest of Hearts Data Protection and GDPR Policy

Responsibilities

Everyone who works for or with Forest of Hearts has responsibility for ensuring any personal data is collected, stored and handled in accordance with this policy and data protection principles.

The MD is ultimately responsible for ensuring that Forest of Hearts meets its legal obligations.

The Data Processing Officer, is responsible for:

- Monitoring compliance with data processing legislation and this policy;
- Regular review and maintenance of this policy and all related procedures;
- Updating the board regarding data protection responsibilities, risks and issues;
- Arranging data protection training and familiarity with this policy, as required, for staff, volunteers and anyone else covered by this policy;
- Handling data protection questions from staff and anyone else covered by
- Dealing with 'subject access requests' from individuals to see the data Forest of Hearts holds about them;
- Checking and approving any contracts or agreements with third parties under which personal data may be handled, exchanged or stored.

The officer is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards, inclusive of any third party services used.
- Performing regular checks and scans to ensure that data security hardware and software is functioning properly.

The officer is responsible for:

- Regular review and maintenance of privacy statements

- Approval of any new or changed consent forms or promotional materials relevant to the use or collection of personal data.

Grounds for Holding Personal Data

In accordance with the Regulations, personal data will only be held in compliance with one of the following Grounds:

- The Data Subject has given clear consent and evidenced for their personal data to be processed for a specified purpose.

- The processing is necessary for a contract placed with Forest of Hearts by the Data Subject, or because they have requested specific steps before entering into a potential contract.

Forest of Hearts Data Protection and GDPR Policy

- The processing is necessary for compliance with a legal or regulatory obligation.

- The processing is necessary for the legitimate interests of Forest of Hearts, i.e. processing that is justified because Forest of hearts' purposes could not be realised without it and could be reasonably expected by the Data Subject.

Principles for Data Access, Retention and Storage

All personnel have a responsibility to uphold the following principles within Forest of Hearts

- The only people able to access data covered by this policy should be those who need it to fulfil their responsibilities.

- All personnel must keep all personal data secure, by taking prescribed precautions including locking computers used to process personal information when unattended.

- When data covered by this policy is stored electronically it must only be stored in a designated manner and protected by strong passwords that are changed regularly and never shared.

- When data covered by this policy is stored on removable media, this must be kept locked away securely when not being used.

- Personal data covered by this policy should never be used on or stored on computers owned by staff or volunteers.

- When personal data is stored on paper, it must be kept where unauthorised people cannot see or access it and when not required should be kept securely in a locked drawer or filing cabinet. When no longer required, such paper records should be shredded before disposal.

- Personal data should not be disclosed to unauthorised people, either within [the Organisation] or externally.

- Personal data should be held in accordance with established and recorded record retention cycles. All such data outside its retention cycle, or otherwise no longer required, should be deleted and disposed of.

- Where personal data is to be transferred externally on an authorised basis it should be encrypted for transmission.

- All personnel must seek advice from their line manager [or officer] if they are unsure about any aspect of data protection.

The officer has a responsibility to ensure that:

- Servers containing personal data and any backup media are located in a secure location.

- All servers and computers containing personal data are protected by approved security software and firewalls.

Forest of Hearts Data Protection and GDPR Policy

Principles for Data Disposal

All personal data will be disposed of by shredding of paper records or deletion from electronic storage. Any electronic storage previously used within Forest of Hearts for holding personal data will be destroyed to the point where data is non-recoverable before disposal.

Principles for Data Accuracy

Forest of Hearts will take all reasonable steps to ensure data covered by this policy is kept accurate and up to date. Accordingly, it is the responsibility of all staff and volunteers to ensure that:

- any item of personal data is held in as few places as necessary.
- every opportunity is taken to ensure data is updated.
- It is made as easy as possible for data subjects to update the information held about them.
- Any item of personal data is updated or removed as soon as any inaccuracies are discovered, eg a stored telephone number is no longer correct.

Principles for Data Disclosure

In certain circumstances, it is permissible to disclose personal data to law enforcement agencies without the consent of the Data Subject.

Under these circumstances, the Data Controller will ensure the request is legitimate, seeking assistance from [the board, legal advisers] as necessary before Forest of Hearts will disclose requested data.

Subject Access Requests

All individuals who are the subject of personal data held by Forest of Hearts are entitled to:

- ask what information Forest of Hearts holds about them and why.
- ask how to gain access to a copy of that data.
- be informed how to keep that data up to date.
- be informed how Forest of Hearts is meeting its data protection obligations.

An enquiry seeking this information is called a ‘Subject Access Request’ and individuals making such an enquiry should be invited to address their request to the Data Controller by

Forest of Hearts Data Protection and GDPR Policy

[letter, email, form on website]. The data controller will aim to provide the relevant data within [Timeframe].

The Data Controller must verify the identity of anyone making a Subject Access Request before providing any information.

Requestors will be charged [Amount] per Subject Access Request, if such a request is 'manifestly unfounded or excessive'.

Management of Consent and Privacy Notices

Forest of Hearts aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, Forest of Hearts has a Privacy Notice, setting out how data relating to individuals is used. This will be made available on request and also be permanently available on the Forest of Hearts website.

The Privacy Notice will be reviewed by The MD at least every two years to ensure that it remains current and accurate.

Where consent is to be obtained from a Data Subject, by electronic or paper based collection there shall be a clear, concise and ambiguous statement, in the form of a mini Privacy Notice, of:

- How the data will be used
- How long it will be retained
- Any intentions to share it
- Forest of Hearts' commitment to secure storage and data protection
- How to access the full Privacy Notice.

The record of consent provided will be retained in parallel with the data provided for the same period of retention and do so securely in accordance with the Regulations.

Management of Breach

Forest of Hearts will ensure that any breach of data protection will be managed in accordance with legislation. Any unauthorised access to, unauthorised alteration of or accidental loss or sharing of personal data will be notified to the Data Protection Officer with immediate effect.

Forest of Hearts Data Protection and GDPR Policy

The Data Protection Officer will initiate an immediate investigation to establish both the cause of the breach and the likelihood and severity of the resulting risk to the rights and freedoms of Data Subject(s).

The Data Protection Officer will, in consultation with Board Members as judged appropriate, determine whether any impact is of sufficient severity to comply with the obligation to notify the Information Commissioner's Office within 72 hours of the breach.

Corrective action will be taken to address identified risks of repeat breaches. If disciplinary action is considered appropriate or complaints/grievances are received, these will be dealt with under the relevant procedures.

Board, Staff and Volunteer Training

Forest of Hearts will ensure that all personnel at every level who are involved in the governance, oversight, management or handling of personal data are appropriately trained to undertake their responsibilities in accordance with this policy.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/]

Signed C Longden Date 12th October 2022 Forest of Hearts