Staple Hill Community Hub
Data Protection Policy (GDPR)

To help protect people's personal data, keep to these Dos and Don'ts:

- Always treat people's personal information with integrity and confidentiality.
- Know what the data protection principles are and apply them.
- Store hard copies securely and transfer them directly to recipients.
- Use secure methods to store and transfer data where needed.
- If you have a work email address and remote access, use it rather than send data to your personal email.
- Be alert to cyber attacks and report suspicious emails or calls.
- Report losses of data or devices as soon as possible.
- Before sending direct marketing, ask the DPO if this is appropriate.
- Take care to use the 'bcc' option for bulk emailing.
- Beware of auto-complete on email. Check you are sending to the right address.
- Ensure your personal device has appropriate security if used for work.
- If you have a question about any data protection issue, ask the DPO.

Summary
Staple Hill Community Hub takes seriously its obligations under the General Data Protection Regulation (GDPR). We are registered with the Information Commissioner. Our registration, which is renewed annually in August, allows us to collect, store and use certain personal information following strict guidelines.

Staple Hill Community Hub needs to collect and use certain types of information about staff, volunteers and the people who come into contact with it in order to carry on our work. This personal information must be collected and dealt with appropriately whether on paper, in a computer, or recorded on other material and there are safeguards to ensure this under the GDPR.

Contents

Staple Hill Community Hub
Data Protection Policy (GDPR)

1 Definitions

The following list below of definitions of the technical terms we have used and is intended to aid understanding of this policy.

Data Controller: A person or organisation that determines how and why to collect and use personal information.

Data Protection Officer: The person(s) responsible for ensuring that Staple Hill Community Hub follows its data protection policy and complies with the GDPR.

Data Subject: The individual whose personal information is being held or processed by Staple Hill Community Hub (for example: a client/service user, an employee, a supporter).

'Explicit' consent is a freely given, specific and informed agreement by a data subject (see definition) to the processing* of personal information* about her/him. Explicit consent is needed for processing sensitive* data.

* See definition

Processing: means collecting, amending, handling, storing or disclosing personal information.

Personal Information: Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual service users, volunteers or employees within Staple Hill Community Hub.

Sensitive data (also known as 'special category data'): Means data about: Racial or ethnic origin; Political opinions; Religious or similar beliefs; Genetics, Biometrics, Trade union membership; Physical or mental health; Sexual life or orientation; Criminal record; Criminal proceedings relating to a data subject's offences.

2 Data Controller

Staple Hill Community Hub is the Data Controller, which means that it determines what purposes personal information held will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

3 Principles of Data Protection

Staple Hill Community Hub regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

Staple Hill Community Hub intends to ensure that personal information is treated lawfully and correctly. To this end, Staple Hill Community Hub will adhere to the Principles of Data Protection, as detailed in the GDPR.

Specifically, the GDPR requires that all personal data is:

1. Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

4. 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.

5. 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.

6. 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.

Staple Hill Community Hub will, through appropriate management, strict application of criteria and controls**:**

- Observe fully conditions regarding the fair collection and use of information.

- Meet its legal obligations to specify the purposes for which information is used.

- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.

- Ensure the quality of information used.

- Ensure that the rights of people about whom information is held, can be fully exercised under GDPR. These include:

    - The right to be informed.
    - The right of access.
    - The right to rectification.
    - The right to erasure (the right to be forgotten).
    - The right to restrict processing.
    - The right to data portability.
    - The right to object.
    - Rights with respect to automated decision-making and profiling.

- Take appropriate technical and organisational security measures to safeguard personal information.

- Ensure that personal information is not transferred abroad without suitable safeguards.

- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.

- Set out clear procedures for responding to requests for information.

4 Data collection

Staple Hill Community Hub will establish there is a need to collect the personal data and will process data only in line with that need.

The GDPR states that the processing of personal data is lawful if the data subject has given consent to the processing of their personal data for one or more specific purposes. As such, data will be collected on the basis of 'informed consent'. Informed consent is when

- A data subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data

- and then gives their consent.

Staple Hill Community Hub will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, Staple Hill Community Hub will ensure that the data subject:

- Clearly understands why the information is needed.

- Understands what it will be used for and what the consequences are should the data subject decide not to give consent to processing.

- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed.

- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress.

- Has received sufficient information on why their data is needed and how it will be used.

- Understands they have a right to be forgotten.

Staple Hill Community Hub will only collect and process personal data for, and to the extent necessary for, the specific purpose or purposes of which the data subject has been informed.

5 Disclosure

Staple Hill Community Hub may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The data subject will be made aware in most circumstances how and with whom their information will be shared.

There are circumstances where the law allows Staple Hill Community Hub to disclose data (including sensitive data) without the data subject's consent.

These are:

1. Carrying out a legal duty or as authorised by the Secretary of State
2. Protecting vital interests of a data subject or other person
3. The data subject has already made the information public
4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
5. Monitoring for equal opportunities purposes – i.e. race, disability or religion
6. Providing a confidential service where the data subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill data subjects to provide consent signatures.

6 Data Storage

Staple Hill Community Hub will ensure that all personal data collected, held and processed is kept secure and that it is managed with integrity.

Data subjects have the right to require Staple Hill Community Hub to rectify any of their personal data that is inaccurate or incomplete. Staple Hill Community Hub will complete the rectification within one month of request.

Data subjects may request that Staple Hill Community Hub stops processing the personal data that it holds about them. In this situation, Staple Hill Community Hub will retain only sufficient date that is necessary to ensure that the personal data in question is not processed further.

6.1 Service Users

Information and records relating to service users will be stored securely and will only be accessible to authorised staff.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately.

It is Staple Hill Community Hub's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

6.2 Staff, volunteers and Trustees

Staple Hill Community Hub holds information about employees to do with their working life in order to fulfil its responsibilities as an employer. Much of this information is personal and Staple Hill Community Hub recognises its duty to

safeguard the data by all means possible and to notify staff about what is kept and why, along with information about how the data can be accessed and by whom.

6.2.1 Information held by Staple Hill Community Hub may include:

- Information relating to recruitment and selection such as application forms; short listing and interview assessments; references; proof of eligibility to work in the UK; where relevant, unspent criminal records and/or the outcome of DBS checks.
- Personal details of name, gender, nationality, date of birth, home address, phone numbers, next of kin.
- Information necessary for payment of salaries, such as bank details, national insurance number, details of deductions to eg the courts or trade unions, expenses claims.
- Information about academic and vocational qualifications and experience.
- Notes of probationary and annual reviews and supervisions.
- Health records including sick notes, and medical assessments and information relating to disabilities.
- Absence records, including sickness absence, compassionate leave, unauthorised absences.
- Time sheets and holiday sheets.
- Details of grievance and disciplinary proceedings including current warnings (within the timescales allowed by the appropriate policies).
- Reference requests and responses.

'Sensitive' data in particular, will only be processed if necessary or advantageous to the employment relationship and with the explicit consent of the individual employee.

Sick notes, absence records and other health-related information are classed as 'sensitive information' and particular care must be taken to ensure that these are stored securely and that access is limited to staff who need to see them.

6.2.2 Why is the information held?

The data kept on staff is primarily in relation to their employment with Staple Hill Community Hub. This data will be used for the purpose of administering and managing their employment.

Information may also be kept for the purposes of applying for funding, obtaining insurance or responding to requests for information from Government departments, the Charity Commissioners or other reputable bodies.

Where possible, sensitive information will not be tied to individuals but will be given in anonymised statistical formats only.

No unrelated data will be kept and any sensitive data (excluding health and criminal records) held by the organisation will be deleted at the request of the individual concerned.

6.2.3 Data Storage

All personnel data is kept either in locked filing cabinets and /or in password protected computer files. Most personal data is kept in individual personnel files in the Staple Hill Community Hub Office cabinet.

Some personal information, including names and photographs, may be published in e.g. newsletters, annual reports, publicity leaflets or the organisation's website. This information will not include home or personal contact details. Staff may request that all or any personal information and/or photographs are restricted to internal access and this request should be complied with.

6.2.4 Consent

Employees give implied consent to Staple Hill Community Hub to hold data as described above and to access and use it as outlined by accepting an offer of employment and agreeing to their Written Statement of Employment Particulars.

Access to staff data is restricted to the Board of Trustees, the Hub manager and the Administrative Assistant.

Information may also be disclosed as required by law, contract or on a 'need to know' basis to trustees, auditors, pension providers, funders, insurers, government departments or other relevant parties/individuals.

Job applicants are also covered by GDPR and by this policy. Staple Hill Community Hub Recruitment Policy and Procedures have been developed to comply with GDPR. Staple Hill Community Hub will only request information which is relevant and not excessive and for the particular purposes of the selection process only. This information will be securely stored and will only be accessed by the Board of Trustees for purposes of administration or selection.

Sensitive information relating to health, disability, criminal records and immigration status will only be requested where necessary for the protection of the organisation and/or its service users and will not be disclosed to anyone who does not need to know.

Sensitive information relating to gender, age, ethnicity and disability may be requested but will be used for equality and diversity monitoring purposes only. This information will not form part of the selection process and will not be retained in any form which identifies the individual to whom it pertains.

The identity of job applicants should be kept confidential as far as possible and for as long as possible. Where a job offer is made, the names of the successful candidates should not be made public until the appointment has been accepted and confirmed.

Feedback on interview performance should be made without specific reference to other candidates.

6.3 Length of time

Staple Hill Community Hub will not keep personal data for any longer than is necessary. Where it is no longer required, all reasonable steps will be taken to remove or dispose of it in a secure manner (eg paper records of personal data will be shredded).

Employees Most information will be retained for as long as a person is employed by Staple Hill Community Hub and for a reasonable period of time thereafter, not exceeding six years.

Job applicants Unsuccessful job applicants data will not be kept for longer than necessary for the needs of the organisation, normally six months.

7 Data access and accuracy

Staple Hill Community Hub will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection.
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice.
- Everyone processing personal information is appropriately trained to do so.
- Everyone processing personal information is appropriately supervised.
- Anybody wanting to make enquiries about handling personal information knows what to do.
- It deals promptly and courteously with any enquiries about handling personal information.
- It describes clearly how it handles personal information.
- It will regularly review and audit the ways it hold, manage and use personal information.
- It regularly assesses and evaluates its methods and performance in relation to handling personal information.
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to criminal or disciplinary action being taken against them.

7.1 Subject Access Requests

All data subjects have the right to make a subject access request ('SAR') to find out about the personal data that Staple Hill Community Hub holds about them, what it is doing with that data and why. Staple Hill Community Hub will comply with requests to access personal data.

Responses will normally be made within one month of receipt, or up to two months if the SAR is complex and/or numerous requests are made. If additional time is required, the data subject will be informed.

Staple Hill Community Hub does not charge a fee for the handling of normal SARs but reserves the right to charge reasonable fees for additional copies of information that has already been supplied to the data subject and for requests that are excessive.

7.2 Service Users

Staple Hill Community Hub will also take reasonable steps to ensure that all personal data collected, processed and held by it is kept up to date by asking data subjects whether there have been any changes.

7.3 Staff, Volunteers and Trustees

7.3.1 Information Technology

Personal data held on computers (including files, emails, databases etc) and personal data downloaded from the web are subject to the same control and restrictions as paper-based data. Staff must take particular care when using any personal data in these contexts. In particular, no personal information should be posted on the internet in any circumstances without compelling reasons and the explicit consent of the individual to whom the information relates.

7.3.2. Monitoring of staff activity

Staff should be aware that Staple Hill Community Hub may, if they have reason to do so, monitor use of the internet and/or emails. Private emails will never be opened intentionally but staff should be aware of the possibility of accidental access and of the Chair of Trustees to question and investigate private use. Deliberate monitoring will only take place where there is good reason to suspect a disciplinary offence or another justified concern.

Performance and quality control monitoring will be overt and for a clear purpose. Covert monitoring will not be permitted.

7.3.3 References

As a matter of good practice, Staple Hill Community Hub will only respond to reference requests that are clearly authorised by the employee concerned. Employment-related references will be provided by the Chair of Trustees. References must be objective, truthful and justifiable.

7.3.4 Subject Access Requests

Staff are entitled to see their own personnel files and to do so, they should arrange a mutually convenient time with the Chair of Trustees. Access may be denied or limited where it involves disclosing information about or from an identified third party (e.g. a colleague) unless the third party concerned has given consent to the disclosure of that information.

As well as taking action to protect third party confidentiality, Staple Hill Community Hub will not respond to subject access requests which:

- disclose any information relating to management forecasts where this could jeopardise the business effectiveness of the organisation;
- or reveal legal proceedings against an individual, except to those directly concerned.

8 Data breach notification

Any personal data breach must be reported immediately to the Data Protection Officer or, in their absence, the Chair of Trustees.

The Data Protection Officer must ensure that the ICO is informed of the breach without delay, and in any event within72 hours after becoming aware of it.

Current guidelines from the ICO will be used to manage these issues.

9 Staff, volunteer and Trustee obligations

The Trustee Board is responsible for notification to the Information Commissioner and should be referred to, along with the Data Protection Officer, with any questions relating to data protection.

However, **all staff** are responsible for ensuring compliance with this policy. They must:

- Ensure that they have read and understood this policy as it relates to them.
- Ensure that data which they supply or for which they are responsible is up-to-date, accurate, fair and relevant to its purpose, including information about themselves. Staff must notify the organisation of any changes in circumstance to enable the organisation to update personnel records accordingly.
- Not keep any records on other individuals (whether other employees or clients/service users) which are unnecessary, incorrect or which contain unfounded opinion or speculation.
- Not share personal information about other members of staff or clients/service users (e.g. sickness, personal circumstances), that they know as a result of handling confidential information (e.g. sick notes, application forms) or which is disclosed in confidential settings (e.g. supervision or counselling), without that person's unambiguous agreement.
- Keep data secure. Paper and external computer files must be locked up, computers must be password protected; laptops and computer disks containing personal information, open computer screens, or open paper files must not be left unattended.
- Not disclose, share or transfer outside the organisation any personal information relating to other staff, volunteers, trustees, or clients/service users without the explicit consent of the individual concerned.
- Dispose of personal data safely. Paper notes and records must be shredded or disposed of as 'confidential waste'. Hard drives of redundant PCs must be wiped clean before disposal.
- Particular care must be taken where personal data is processed 'off-site', at home or in other locations. This presents a greater risk of loss, damage or theft and staff must take appropriate security precautions.

10 Implementation

The Trustee Board is responsible for the implementation of this policy.

11 Contacts

In case of any queries or questions in relation to this policy please contact Staple Hill Community Hub.

Staple Hill Community Hub Data Protection Officer: Julie Snelling

12 Review

This policy will be reviewed every three years, or earlier if circumstances warrant it.