Data Protection Policy

Our data protection policy sets out our commitment to and legal requirements for protecting the personal data we process, and how we implement that commitment with regards to the collection and use of personal data.

It also covers everyday procedures for ensuring good practice in handling, storing and protecting personal and sensitive data.

Principles

Mentoring Plus needs to keep certain information on its employees (including applicants), volunteers, service users, service user families, referrers, suppliers, delivery partners, trustees, funders and donors to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the Data Protection Act (DPA) 2018. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

1. Personal data – legal requirements

In line with the Data Protection Act 2018 principles, Mentoring Plus will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specific and lawful purpose
- Be adequate and relevant but not excessive
- Be accurate and kept up to date
- Not be held longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures
- Not to be transferred outside the European Economic Area (EEA).

The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes paper-based personal data as well as that kept on computer.

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e.

- *Accountability:* those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.

- *Visibility:* Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected or deleted and to know who has had access to this data.
- *Consent:* The collection and use of personal data must be fair and lawful and in accordance with the DPA's eight data protection principles. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.
- *Access:* Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.
- *Stewardship:* Those collecting personal data have a duty of care to protect this data throughout the data life span.

2. Governance

As a non-profit organisation holding data about a defined membership, Mentoring Plus is currently exempt from notifying the Information Commissioner about the needs we have for processing personal data and our designated Data Controller. We review these guidelines on an annual basis and will notify the Information Commissioner in future if the law requires.

Under the Data Protection Guardianship Code, overall responsibility for personal data in a voluntary organisation rests with the governing body. In the case of Mentoring Plus, this is the Board of Trustees.

The governing body delegates tasks to the Data Controller. The Data Controller is responsible for:

- understanding and communicating obligations under the Act
- identifying potential problem areas or risks
- producing clear and effective procedures
- notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes, where relevant.

All employed staff and any volunteers who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

Breach of this policy will result in disciplinary proceedings for employed staff, including for breaches of adequate supervision of volunteers.

To meet our responsibilities, staff and any volunteers working under staff supervision will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised

We will ensure that:

- Everyone managing and handling personal information is trained to do so.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in line with our procedures.
- Queries about handling personal information will be dealt with swiftly and politely.

3. Training and awareness raising

Training and awareness raising about the Data Protection Act and how it is followed in this organisation will take the following forms:

On induction: This policy, alongside our Data Security policy and any other guidelines in force are shared with the staff member. Recipients sign for information received as proof of receipt, understanding and commitment. New staff members are trained regarding secure and private passwords, physical data storage in locked files, the location of keys etc.

General training/ awareness raising: This policy alongside all our policies are updated and distributed to all staff annually.

4. Data subject consents

Collecting personal data and consents
Before personal information is collected, we will consider what details are necessary for our purposes and how long we are likely to need this information. Types of data held and our retention policy for each are set out in the Data Retention Appendix available on request.

The documents used to collect information will clearly set out for people whose information is gathered the following:

- why the information is being gathered
- what the information will be used for
- who will have access to their information (including third parties where relevant).

Where necessary, we will seek explicit and dated consent from data subjects for us to hold and process their data for the purposes stated, and state our commitment to protect their data in line with this policy.

Data and consent updates
To ensure that personal information kept is accurate, for data which has been held for more than 24 months, a reminder will be sent to people to check and confirm their details and their consent for us to hold it for the purposes stated.

Where these are not returned we will remove their details. In exceptional cases where we judge that these individuals will lose out on positive opportunities by removing their details, we will hold them securely for another 6 months issuing follow-up reminders before they are removed.

Personal sensitive information
Personal sensitive information will not be used apart from the exact purpose for which +-permission was given. If we are asked to share personal sensitive information for any other purpose, we will obtain explicit, informed consent before doing so. This includes ethnic origin, political opinions, religious beliefs, membership of a trade union, physical or mental health, criminal convictions etc.

Sharing of information
In the case of service users, their families and volunteers, we will inform them at the outset that we are required to hold information for a stated length of time, and of the circumstances under which we will have to share sensitive information e.g. a serious case review or council freedom of information request (see below). If individuals have requested data deletion, they will be informed that redacted information which cannot identify them may be held and shared for the required length of time in order to allow us to comply with this requirement.

Data disposal
Mentoring Plus will ensure that information is kept according to retention periods set out in the Data Protection Appendix available on request, and securely disposed of thereafter. Data review and disposal processes will be implemented at least every 3 months, so that deletion will occur within 3 months of the relevant consent and/or retention period ending.

5. Sharing data with partners

Mentoring Plus delivers projects in partnership with a number of organisations. Partnership agreements for all projects involving young people and/or volunteers contain reference to information sharing protocols and requirements. They include:

- Consent
- Staff and others with access to information
- Data Protection Act notification
- Subject access requests
- Freedom of Information
- Records management
- Information security
- Dealing with concerns and complaints.

6. Freedom of Information (FOI) Act 2000

Statutory authorities and other public bodies are required to respond to requests under the Freedom of Information (FOI) Act 2000. In some cases Mentoring Plus may hold relevant information and be approached for information by a statutory authority with which it has a supply contract.

Mentoring Plus will require full details from the statutory authority about the nature of the request and the information required, in order to make a decision about whether or not Mentoring Plus is willing to provide the information. Requests should be made by the statutory authority to the appropriate Mentoring Plus lead within 28 days of receiving the request from the member of the public.

Mentoring Plus will require time to consider the request and to locate the relevant information, where available, as appropriate. Decisons about whether or not to disclose will be made within 10 working days and the relevant information passed on (if appropriate) within a further 10 working days of the request being made to Mentoring Plus.

7. Sharing information with data subjects

Anyone whose personal information we process has the right to know:

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to the CEO of Mentoring Plus at our published address.

The following information will be required before access is granted:

- Full name and contact details of the person making the request
- Their relationship with the organisation (former/ current member of staff, trustee or other volunteer, service user, etc)
- Any other relevant information, e.g. timescales involved.

We may also require photographic and address proofs of identity before access is granted, in forms as currently acceptable for DBS applications.

Queries about handling personal information will be dealt with swiftly and politely. We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 40 days required by the Act from receiving the written request.

8. Keeping data secure

The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.

Personal information may be stored:

- in hard copy files in locked filing cabinets and drawers
- on a shared computer network hosted by an authorised supplier with access protected by individual secure user passwords and backed up to a secure cloud server
- on a cloud-based online database hosted by an authorised supplier with access protected by individual secure user passwords.

Sensitive personal information such as equal opportunities data, DBS disclosures and similar is stored as above and accessed only by trained members of staff.

People within the organisation who will process personal information are limited to trained staff.

In the rare situation where volunteers are asked to assist in processing personal information, this is under the direct supervision of a staff member and following training and a volunteer agreement including full confidentiality and data protection procedures. The staff member supervising is responsible for the volunteer's compliance.

For hard copy materials, all staff:

- Only keep paper copies of materials if strictly necessary e.g. those which have to be collected or referred-to in hard copy during meetings
- Maintain a single structured filing system for all staff so that hard copy materials are easily located and kept updated
- Keep all materials containing personal data in secure filing storage, which is locked at any time when the office is not staffed
- Materials containing personal data are not left on desks, shelves or filing trays at any time
- The doors of the offices in which hard copy materials are stored are locked when unoccupied, with keys/entry code being kept only by authorised staff members
- Ensure the building and car park are securely locked out of office hours and a regularly maintained alarm is set
- Accompany visitors on and off the premises, and do not give any visitor unsupervised access to the computer network or file storage areas

- Review files at least annually, and with appropriate authorisation, securely dispose of materials that do not need to be kept or which should be disposed of as set out above.

For data stored electronically:

- Firewall, virus-checking and anti-spyware software is installed and kept regularly updated on all computers
- Computer applications in use on computers are kept updated, with the latest patches or security updates installed to cover vulnerabilities
- Staff only access information they need to do their job
- Staff use a strong password which is regularly changed and do not share passwords with each other. Network passwords can only be accessed with the help of our contracted external IT support agency to ensure business continuity (see below)
- Laptops, mobiles and other devices are stored securely when off site, strongly password protected, and never used to store personal data on a local drive
- Data sticks or similar are not used to store personal data at any time
- Any personal information held electronically that would cause damage or distress if it were lost or stolen is password protected and/or encrypted
- All personal information is removed before disposing of old computers (by expert suppliers using appropriate technology or destroying the hard disk)
- Backed up information on our cloud server can only be accessed by skilled and authorised IT support
- Staff are trained to access our cloud server remotely only through secure devices and adequately protected user accounts, and never to save personal data on local devices.

To ensure email use does not compromise data security, all staff:

- Consider whether the content of the email should be encrypted or password protected.
- Take careful note that the correct recipient is addressed
- Ensure a recipient whose address should not be revealed to other recipients is blind carbon copied (bcc), not carbon copy (cc).
- Take appropriate care when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.
- Only send a sensitive email if you know the recipient's arrangements are secure enough before sending your message
- Are aware of the risk of 'phishing' attacks from fraudulent parties asking for any form of personal, password or financial data, their own or others'
- Do not open spam messages; delete immediately
- Never open attachments from unknown senders or where the attachment from a known sender is not identified or looks in any way suspicious
- Do not send or forward emails which could possibly be construed as compromising personal data, being offensive or inappropriate, or risking the reputation of the organisation. Consider all the individuals who may see an email inadvertently (such as children on a shared home computer), not just the immediate addressee.
- Anonymise personal details contained in an email e.g. including only initials
- Only share sensitive information with statutory colleagues securely via Globalscape or similar encrypted systems.

Additionally, appropriate training is undertaken to ensure staff:

- Never disclose personal data to third parties unless explicitly authorised to do so
- Always ask questions so they can be reasonably assured that the caller is genuine
- Establish what information is required - establish whether the caller is entitled to the information, and if in doubt, do not disclose
- Be especially cautious if the caller is not the data subject
- Never discuss/disclose sensitive information such as medical history.

Any unauthorised disclosure of personal data to a third party by an employee may result in disciplinary action, including disclosure by a volunteer under their supervision.

9. Data and business continuity

For data security and business continuity in the event of data being lost due to premises or IT damage, we ensure that:

- Critical data is held on a remote and secure database on a secure cloud server.
- A master file of business-critical and contact information is maintained in hard copy where it can be readily accessed in the event of office evacuation, and a copy kept securely offsite
- Staff are aware of response procedures in the event of office premises being unusable, including contact numbers and priority actions, and are able to carry out all key tasks working remotely
- In the event of damage to office premises, all materials still stored there are appropriately moved and/or secured as soon as it is safe to access the building.

10. Data security breach

In the unlikely event of a data security breach, the following actions are immediately carried out under the direction of a responsible officer:

- *Containment*: immediately ensure that no further breaches can occur e.g. by securing hard-copy materials, having IT systems expertly checked for malware, implementing changes and changing passwords.
- *Assessment of the risks*: immediately establish what data has been compromised and the specific risks associated with this breach. Evaluate the potential adverse consequences for individuals based on these specifics; how serious or substantial are these risks and how likely they are to happen.
- *Damage limitation*: inform those individuals potentially affected (their parents where data affected pertains to under-18s) and ensure they are aware of their need to take appropriate steps such as monitoring communications and changing passwords.
- *Wider notification of breach*: based on the assessed risks, a responsible officer then determines whether it will aid damage limitation if other parties such as the police, other relevant agencies or the media are informed, and implements decisions accordingly.
- *Evaluation and response*: investigate the causes of the breach and the effectiveness of the response to it. Update policies and procedures accordingly.

When a breach of data protection occurs, consideration will be given to reviewing practices. In addition, Mentoring Plus will consider whether the breach should be reported to the

Information Commissioner and/or to any partners with which we hold Information Sharing or Partnership Agreements.

11. Review

This policy will be reviewed annually to ensure it remains up to date and compliant with the law.

Staff compliance

I confirm I have read and understood Mentoring Plus' Data Protection Policy and will act in accordance with it.

I am connected with this organisation in my capacity as _ _____

Signature:

Print name:

Date:

Please return this form to Ruth Keily, CEO

Last reviewed: September 2024
Next review: September 2025