



Data Protection Policy

This policy takes account of UK and EU law and conventions and specifically to address the General Data Protection Regulations 2018 (GDPR).

Data protection policy

Anyone who obtains personal information (“data”) about other individuals is a ‘data controller’ and is thus regulated by the Data Protection Act 1998 and the GDPR. The legislation controls what can lawfully be done with information and gives individuals certain rights to control how information about them is obtained, used, stored and distributed. These rights include the right to find out what information a data controller has about them, and ask for copies of data. There is also now an enhanced set of Individual Rights that an organisation needs to respect.

We are a data controller in relation to all the information that the organisation obtains about employees, agency workers, suppliers, service users, residents and customers.

We will seek employees’ and volunteers specific consent to the organisation processing data in whatever format including sensitive personal data about their employment or use. Personal data, including sensitive data, may be collected for statistical purposes (e.g. equality and diversity, absences, turnover) or to enable health and safety or employment and pay obligations to be met, or to schedule volunteers’ involvement.

We must be able to demonstrate that any personal data we handle is:

- processed lawfully, fairly and transparently
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and kept up to date where necessary
- kept for no longer than is necessary where data subjects are identifiable
- processed securely and protected against accidental loss, destruction or damage.

We are committed to following these principles. Data will be retained as necessary during the course of an individual’s employment and records will be retained for up to six years after the data that they leave the employment in case legal proceedings arise during that period.

Data will only be retained for a period of longer than six years if it is material to legal proceedings or should otherwise be retained in our interests after that period.

Data will be kept in a secure system whether manual or computerised to the best of our ability at all times. When transmitting data this will be password protected and/or encrypted.

The Act prohibits the transfer of data outside the European Economic Area to countries that do not have similar protection of data except in some circumstances or with the subject’s consent. Mind BLMK has no intention of sharing personal data outside the UK.

Access to data

The HR and Systems Manager, Sonnet Church (sonnet.church@mind-blmk.org.uk), will act as a **Data Protection Compliance Officer**.

A request for access to any personal data that relates to an individual will be made by a written request using the Data Access Request form and the originator's details will be verified. The completed form must be returned to the Data Protection Compliance Officer. There may be fees chargeable for this.

Employees' and volunteers' consent will be obtained where the organisation is making personal data / information available to those who provide services to the organisation (such as HR advisors), regulatory authorities, governmental or quasi-governmental organisations and potential purchasers of the organisation or any part of its business. Similarly consent will be sought to the transfer of personal information to business contacts outside the European Economic Area in order to further the organisation's business interests.

Where contractors are used to obtain, record, store or process personal data on behalf of the organisation, that service provider will only be commissioned or have a contract renewed if they meet data protection quality assurance standards set by us, so that they can demonstrate compliance with the DPA and GDPR.

There may be certain circumstances where a person's consent cannot be obtained or is not legally required. Before releasing personal data to external organisations (including the police) the organisation will seek to obtain legal advice on its obligations and where necessary ask for a court order or a magistrates warrant before release of personal information about employees, volunteers, service users or suppliers.

The organisation's policy is to provide copies of all data that the organisation is obliged to disclose within 28 days of receipt of a request being received by the Data Protection Compliance Officer.

The organisation considers that if a period of less than one year has elapsed since any previous request for access to data was complied with, it is not reasonable to expect us to be obliged to comply with a further request before a year has elapsed unless there are exceptional circumstances.

It is our policy to ensure that all data is as accurate as possible and all necessary steps to ensure that this is the case and to rectify any inaccuracies will be taken. See **Individuals' Rights** below.

Where we have requested an employment reference in confidence from a referee and that reference has been given on terms that it is confidential and that the person giving it wishes that it should not to be disclosed, it is our policy that it would normally be unreasonable to disclose such a reference to others unless the consent of the person who gave the reference is obtained.

For the purposes of the DPA and the GDPR data is any personal information that is collected on an individual for whatever purpose and which is then recorded, processed or stored in some way for legal, business, technical or organisational reasons.

The information can be paper-based and filed manually, or electronic and saved on computerised systems or in a "cloud" database. The GDPR extends this to include biometric or visual images that can identify a person, and any automated processing that takes place.

We will undertake an audit of all types of data collection, recording and processing taking place and repeat this on an annual basis. We will review the reasons for the data being obtained and justify why this should continue, or make a decision it will no longer be obtained.

Similarly we will review the way in which the data is stored and processed to ensure all appropriate safeguards are in place and security/confidentiality measures are effective.

We will:

- carry out a risk assessment of data systems and act on the results

- maintain up-to-date security systems (for example, using firewalls and encryption technology)
- restrict access to personal data to only those who demonstrate that they need it
- train staff on data security
- review data security regularly

We will publish an annual report on data protection and the measures taken to comply with legislation and individual's rights.

Individuals' rights

While many of these rights are similar to those under the current DPA, the GDPR expands them and introduces new ones. Data subjects, including employees, will have the:

- **right to be informed about the processing of their personal data** – the Guidance on Data Protection and this document sets out how the organisation is complying with the data protection requirements for the processing of personal data.
- **right to rectification if their personal data is inaccurate or incomplete** - on a regular basis employees and volunteers will be asked to re-confirm or to amend the personal data kept. Requests to amend data will normally have to be processed within one month.
- **right of access to their personal data** and supplementary information, and the right to confirmation that their personal data is being processed - a statement will be provided to each employee and volunteer setting out what personal data is being collected, recorded and processed and why, also who has access to their personal data.
- **data subject access requests (SARs)** an employee or volunteer can at any time request access to their personal data and a process for such requests will be devised. A SAR will be responded to within one month of receipt (as per GDPR requirements).
- **right to be forgotten** by having their personal data deleted or removed on request where there is no compelling reason for an organisation to continue to process it - when the employee or volunteer receives their statement on what personal data is being collected they will be given the opportunity to challenge any data held on them and ask for its removal.
- **right to restrict processing of their personal data**, for example, if an employee consider that processing is unlawful or the data is inaccurate - as for the right to be forgotten.
- **right to data portability of their personal data** for their own purposes (employees will be allowed to obtain and reuse their data) – data will be kept in a format capable of portability/transferability.
- **right to object to the processing of their personal data** for direct marketing, scientific or historical research, or statistical purposes - as for the right to be forgotten.

Consent

Each employee and volunteer will, on being given their Personal Data Statement, also be asked to give consent to the specific data being collected, stored, recorded and processed, or a legal basis for the information being obtained for which no consent is needed explained.

Breach of data protection policy or legal requirements

Any suspected or actual breach of this policy whether direct or indirect, malicious or unintentional must be reported immediately to the Data Protection Compliance Manager and the ICO (Information Commissioner's Office) informed.

The organisation will implement its **Contingency Plan** in order to immediately protect personal data and resolve the cause of the breach.

We will consider any serious breach of the policy and data protection rules to be Gross Misconduct for which the normal penalty will be summary dismissal.

The following elements are where we feel there may be an impact on the DPA/GDPR compliance requirements and therefore should be part of this policy.

Surveillance

We may have a CCTV systems on premises to assist with maintaining the security of the business. There will be no covert operation of this system and all camera sites will be clearly visible.

No covert video or audio recording of the workplace or workers, including at an employee's home (e.g. to verify reasons for absence) will take place for management purposes and this will only be used if part of a legal investigation into criminal activities. No video or audio recording will be released to third parties unless specific consent has been obtained or a court order or warrant has been issued by regulatory authorities including the police.

Contacting workers outside of working hours or while absent from the workplace

Employees and volunteers have a right to privacy outside of the workplace and this will be respected and representatives of the organisation will not access personal data to routinely contact workers by telephone, email, social media or face to face unless by consent or within the terms of the employment relationship (e.g. home working). This applies to off-shift time or outside normal working hours, weekends or while the employee is on authorised holiday.

However there will be circumstances where a manager or Director will want to contact an employee, volunteer or a member of their family - in an emergency situation, when an employee or volunteer has vital organisational information that is required immediately, when no contact has been received from an individual and a manager needs to check what the position is, as part of absence management, or when a manager or Director is concerned about the employee's health and wellbeing.

Confidentiality

Employees and volunteers must not disclose any information of a confidential nature relating to the organisation's business to any other party without express authority from a senior manager. This extends also to the disclosure of confidential personal data of other employees, agency staff, customers, suppliers or contractors.

Employees and volunteers are not allowed to remove any documents or tangible items which contain any confidential information or intellectual property from the premises at any time without proper advance authorisation, this will include computer files, records and other equipment that can be used to store information. If authorised to do so, employees and volunteers must safeguard the information and follow the Data Protection Act /GDPR principles.

Upon the termination of employment, all documents and tangible items which belong to the organisation or which contain or refer to any confidential information must be returned by the employee.

Subject to legal requirements or court orders, all confidential information from any re-usable material will be deleted upon a senior manager's instruction and all other documents and tangible items which contain or refer to any confidential information will be destroyed. This will include computer files, discs and removable drives.

Use of computers

Employee and volunteers use of the organisations computers and other devices is normally restricted to business reasons, and any personal information they choose to upload or any use made by an individual of the computer or device for non-business reasons could be monitored and accessed by managers. Employees should therefore be made aware that their personal information and use cannot be considered to be confidential in these circumstances.

In order to maintain the integrity of computer system and records and to protect the confidentiality of any personal data, the following rules must be observed:

- Passwords for access to the system are confidential and must not be revealed to other persons. They should be changed regularly.
- All software or disks must be authorised by a Manager before they are loaded onto or even placed in any computer.
- Upon the discovery of computer virus and/or corrupted information, a Manager must be advised immediately.
- The creation, generation, and distribution of materials that are offensive on race, sex, sexual orientation, transgender, disability, age or religious grounds are forbidden.
- It is forbidden to use the computer system to generate and/or distribute material which is offensive to or ridicules other employees.
- The storage of any kind of offensive material (including pornography) on the computer system is expressly forbidden.
- In respect of these rules material will be considered offensive if it causes distress to the person who receives or discovers it.
- We will consider any serious breach of these rules to be Gross Misconduct for which the normal penalty will be summary dismissal.

Internet and social media sites

We recognise that in their private time employees may wish to publish content on the internet through a variety of means. Even outside of work employees must adhere to the following guidelines when creating, modifying or contributing to websites.

a. Social networking

- The growth of computer use and internet expansion has led to an increase in the use of blogs and social networking sites. Whilst employees may choose to indulge in this practice at home the company has strict guidelines on the use of such sites.
- The use of social networking sites and blogs must not be allowed to interfere with or bring into disrepute the conduct of the organisation or its name or reputation.
- No personal blogs or social networking profiles whatsoever will be created or updated on ANY computer owned and operated for the organisation's business.
- No employee must directly or indirectly refer to or implicate the organisation, its employees or any of its customers /service users on any blog or social networking profile created by them.
- If, in any contribution or posting which identifies or could identify the individual as an employee, agent or other affiliate of the organisation, the employee expresses an idea or opinion, he/she should include a disclaimer which clearly states that the opinion or idea expressed is that of the individual and does not represent that of the organisation.
- Employees will be made aware that harassment, defamation and libel laws cover what is said and written on social media and if an individual feels that they have been harassed, bullied or discriminated against. Legal action can be taken against the perpetrator including the involvement of the police.

We consider any serious breach of the above guidelines to be Gross Misconduct which may result in summary dismissal.

b. Email /SMS code of conduct

Bullying, harassment or abuse of others through the use of e-mail or SMS is forbidden. This includes sending information that insults or harasses others with respect to sex, sexual orientation, transgender, race, age, disability or religion.

It is forbidden to:

- access or distribute pornography;
- post confidential information about Mind BLMK, its employees, service users or suppliers without authorisation.

When replying to an e-mail or SMS, make sure that the reply is for the sender only and not the original mailing list (unless there is a requirement to do so).

Files that have hidden confidential information (e.g. base cost calculations you may have used to generate a quote) should only be sent if within the Data Protection Principles and this policy. In any case attachments of a sensitive nature should be password-protected or encrypted.

Should employees or a volunteer be subject to harassment or abuse from e-mail or SMS at work from another employee or volunteer, or service user, then the matter should be reported through the Grievance Procedure immediately.

Equality, diversity and inclusivity

The use of personal data and images in whatever format to discriminate, bully, harass or victimise another person be it an employee or not, or using personal data to violate someone's Human Rights will be treated as gross misconduct and may also leave the organisation and the individuals involved open to criminal and/or civil legal proceedings.

Please read the organisation's full Single Equality Scheme.

Protection against detriment

Employees and volunteers will not suffer any detriment, or penalty for challenging the personal data we hold on them or the processes involved, for making subject data access requests or refusing consent to the obtaining, recording or processing of a the individual's personal data.

Anyone concerned about the legal status or ethical use of anyone's personal data by the organisation should report this immediately to the Data Protection Compliance Officer.

Last review date:	n/a (new policy)
Next review date:	May 2021
Lead:	HR and Systems Manager
Overseeing Committee / Management Group:	Exec
Approval Date:	08.05.14
Review cycle:	3 yearly and/or as per legislation changes