Date adopted	**February 2018**
Last Review	**May 2018**
Next Review	**May 2021**
Author	**Michelle Kabia**

General Data Protection Policy

1. Introduction

1.1 About this policy

This policy sets out how Mind in Tower Hamlets and Newham seeks to protect personal data of our staff and service users. It will ensure that staff understand the rules governing their use of personal data to which they have access to in the course of their work. In particular, it emphasises that the policy requires the organisation to consult the Privacy Impact Assessment when designing new services to ensure that relevant compliance steps are addressed.

1.2 GDPR

The General Data Protection Regulation (GDPR) is a regulation by which the EU intends to strengthen and unify data protection for individuals within the EU, replacing the Data Protection Act (DPA). Organisations must be compliant from the 25th May 2018.

New elements and enhancements aim to create greater consistency between organisations, clearer consent, ensure data protection by design, invoke stronger penalties, mandatory breach reporting and enhancements on the protection and use of the subject's data, for example, the right to be forgotten.

1.3 Definitions:

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll, and business development purposes. Business purposes for Mind in Tower Hamlets and Newham includes the following: - Compliance with our legal, regulatory and corporate governance obligations and good practice - Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests - Ensuring business policies are adhered to (such as policies covering email and internet use) - Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking - Investigating complaints - Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments - Monitoring staff conduct and disciplinary matters

	- Marketing our business - Improving services
Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers, volunteers and marketing contacts. *Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, CV, and client-related information such as doctor details and selection status..*
Sensitive personal data	Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, sexuality, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.

2. Data Processing at Mind in Tower Hamlets and Newham

2.1 Who is in charge of data?

We have considered whether we are required to formally designate a Data Protection Officer who is external to our organisation, but have concluded that we do not carry out processing on a large enough scale to warrant this.

The CEO and HR Manager will ensure that the board is kept updated about data protection responsibilities, risks and issues.

Data protection procedures and policies will be reviewed on a regular basis.

2.2 Processing data

In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

2.3 Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the CEO and/or HR manager.

2.4 Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform CEO and/or HR manager so that they can update your records.

2.5 Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the CEO and/or HR manager will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

2.6 Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The CEO must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

2.7 Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Physical data must be stored in locked cupboards or filing cabinets.

2.8 Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the CEO and/or HR manager.

3. Subject Access Requests

Under GDPR individuals are entitled, subject to certain exceptions, to request access to information held about them. If a member of staff receives a subject access request, they should refer that request immediately to the HR manager. They may need to assist complying with those requests.

3.1 Processing data in accordance with individual rights

We will abide by requests from individuals not to use personal data for direct marketing purposes. The HR Manager and CEO, and any other relevant managerial staff, will be notified about any such request.

We will not send direct marketing material to anybody electronically unless we have an existing business relationship with them in relation to the services being marketed.

3.1 Training

All staff and trustees will be required to complete the GDPR training on Me Learning to support their understanding of the new Data Protection Guidelines.

4. GDPR Provisions

The following provisions will be in effect on or before 25 May 2018.

4.1 Privacy Notice

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation.

Privacy Notice

Here at Mind in Tower Hamlets and Newham we take your privacy very seriously and only use your personal information to provide the services you have requested from us.

Your information will be used by our staff and volunteers so they can support you. We may also get information about you from partner organisations, or give information about you to them. We will only do this when service contracts require it. We may share information with legal and regulatory authorities if required to by law.

Your communications with our teams (including by telephone or email) may be monitored and/or recorded for training, quality control and compliance purposes to ensure that we continuously improve our service provision.

We take the security of your personal information extremely seriously and have implemented appropriate measures to protect the personal information we have under our control.

We fully comply with our legal obligations as a data controller, and you can change your mind and remove consent at any time by contacting us at info@mithn.org.uk.

4.2 Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

4.3 Justification for personal data

We will process personal data in compliance with all six data protection principles.

We will document the additional justification for the processing of sensitive data, and will ensure any biometric and genetic data is considered sensitive.

4.4 Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

4.5 Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

4.6 Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

4.7 Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

4.8 Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The CEO will be responsible for conducting Privacy Impact Assessments and ensuring that all new services commence with a privacy plan.

4.9 Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

4.10 Reporting breaches

ICO requires breaches to be reported within 72 hours. All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the CEO of any compliance failures that are material either in their own right or as part of a pattern of failures
- If a staff member becomes aware of a data breach out of work hours, they should advice their line manager immediately

4.11 Monitoring

Everyone must observe this policy. The CEO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

5. Failure to comply

We take the privacy of our staff and service users seriously. Failure of staff to comply with this policy may lead to disciplinary action for staff and/or the organisation.

mind for better mental health in Tower Hamlets and Newham

Consent Form

Mind in Tower Hamlets and Newham is committed to protecting and respecting your privacy and personal data, in line with the General Data Protection Regulations (GDPR). Please refer to our General Data Protection Policy for more information.

Data collection and Storage

We gather and securely store information about you to enable us to provide you with the service(s) that you need. Some of our services are delivered in partnerships with other organisations, and where necessary to the service(s) you require your information will be shared with relevant partners.

Confidentiality

All staff and volunteers across our organisation and our partner organisations are bound by confidentiality agreements. We would only share your information with third parties if required to do so to maintain your safety, the safety of others or if required to do so by law, for example by a court. In these cases we would only disclose the personal information necessary to ensure that you receive the support you need.

Right to access your information

You have the right to request access to the information we hold about you at any time, free of charge. We will be able to comply with this with 10 days notice.

Right to have information held on you removed

You have the right to remove your consent at any time and have any information we do not need to keep by law removed from our records. There are some circumstances where we are required to retain data by law. If this is the case then we will retain the information however we will remove your identifying details from the record.

Consent

Please tick the boxes and sign below to consent to:

☐ The personal data you provide us with being securely stored and shared as set out above, as necessary to the service(s) you require

☐ Being contacted by Mind in Tower Hamlets and Newham or relevant partner organisations by phone or email in relation to the service(s) you require

Name:

Signature:

Date:

If consent given over the phone:

Staff Signature:

Date: