MIND IN KINGSTON DATA PROTECTION POLICY

A) INTRODUCTION

Mind in Kingston collects and uses information about people with whom we work. This personal information must be handled and dealt with properly, regardless of how it is collected, recorded and used, and whether it is on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important for Mind in Kingston to operate successfully and to maintain confidence between us and the people who we work with. We will ensure that we treat personal information lawfully and correctly.

To this end we have adopted and comply with the Data Protection Act 2018, which sets out the principles of the General Data Protection Regulation (GDPR).

This policy applies to the processing of personal data in manual and electronic records kept by us for HR (Human Resources) purposes, and in connection with the services we deliver, as described below. It also covers our response to any data breach and other rights under the GDPR.

This policy applies to the personal data of job applicants, existing and former employees, agency workers, contractors, apprentices, trustees, volunteers, and placements. These are referred to in this policy as staff.

It also applies to personal data of beneficiaries, their carers, family members, friends, professionals and others involved in their care. These are referred to in this policy as *relevant individuals*.

B) DEFINITIONS

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for ID purposes, health data, sex life and sexual orientation.

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

C) DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) processing will be fair, lawful and transparent
b) data be collected for specific, explicit, and legitimate purposes
c) data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
d) data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
e) data is not kept for longer than is necessary for its given purpose
f) data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
g) we will comply with the relevant GDPR procedures for international transferring of personal data

D) TYPES OF DATA HELD

We keep several categories of personal data on our staff in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each member of staff and we also hold the data within our computer systems.

Specifically, we hold the following types of data:

a) personal details such as name, address, phone numbers and email address
b) information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter, references from former employers, details on your education and employment history etc
c) details relating to payroll such as National Insurance numbers, bank account details and tax codes
d) medical or health information
e) information relating to your employment with us, including:
    i) job title and job descriptions
    ii) your salary
    iii) your wider terms and conditions of employment

iv) details of formal and informal proceedings involving you such as letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal and performance information
v) internal and external training modules undertaken

We also keep data on our beneficiaries. This data varies according to the service they use and how long they interact with us. We keep this data in files relating to the service, and we also hold the data within our computer systems.

Specifically, we hold the following types of data:

a) personal details such as name, address, phone numbers and email address
b) where beneficiaries are also tenants, bank details and housing benefit information
c) information about their mental health and/ or other conditions
d) information about financial circumstances (such as debt and benefit information)
e) other information relevant to casework, such as supporting statements or letters, employment details

All of the above information is required for our processing activities. More information on those processing activities are included in our privacy notice for staff, which is available from a member of staff's line manager. For beneficiaries, we have included information about these activities in the privacy notice for beneficiaries which can be obtained from the person undertaking case work with beneficiaries. There is also a separate policy for Beneficiaries which staff can share with the people they work with.

E) INDIVIDUAL RIGHTS

You have the following rights in relation to the personal data we hold on you:

a) the right to be informed about the data we hold on you and what we do with it;
b) the right of access to the data we hold on you. More information on this can be found in the section headed "Access to Data" below and in our separate policy on Subject Access Requests";
c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
d) the right to have data deleted in certain circumstances. This is also known as 'erasure';
e) the right to restrict the processing of the data;
f) the right to transfer the data we hold on you to another party. This is also known as 'portability';
g) the right to object to the inclusion of any information;

h) the right to regulate any automated decision-making and profiling of personal data.

More information can be found on each of these rights in our separate policy on relevant individuals rights under GDPR.

F) RESPONSIBILITIES

To protect the personal data of relevant individuals, those within Mind in Kingston who must process data as part of their role, have been made aware of and have had training in our policies on data protection.

We have also appointed staff with responsibility for reviewing and auditing our data protection systems.

G) LAWFUL BASES OF PROCESSING

We acknowledge that processing may be only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

Where no other lawful basis applies, we may seek to rely on the member of staff's consent in order to process data.

However, we recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. Members of staff will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

H) ACCESS TO DATA

As stated above, relevant individuals have a right to access the personal data that we hold on them. To exercise this right, relevant individuals should make a Subject Access Request. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the member of staff making the request. In these circumstances, a reasonable charge will be applied.

Further information on making a subject access request is contained in our Subject Access Request policy.

I) DATA DISCLOSURES

Mind in Kingston may be required to disclose certain data/ information to another person or another company. For people working for us, the circumstances leading to such disclosures include:

a) any staff benefits operated by third parties;
b) disabled individuals - whether any reasonable adjustments are required to assist them at work;
c) individuals' health data - to comply with health and safety or occupational health obligations towards the member of staff;
d) for Statutory Sick Pay purposes;
e) HR management and administration - to consider how an individual's health affects his or her ability to do their job;
f) the smooth operation of any member of staff insurance policies or pension plans;
g) to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.

These kinds of disclosures will only be made when strictly necessary for the purpose.

For beneficiaries, the circumstances leading to such disclosures include:

a) acting on behalf of an individual, where consent has been given
b) for safeguarding purposes where an individual is deemed at risk
c) where disclosure is required by law, such as the prevention or detection of a crime
d) where the health and wellbeing of an individual is at risk

These kinds of disclosures will be requested by the member of staff dealing with the individual and authorised by their line manager and recorded in their file. Mind in Kingston will only disclose the minimum necessary data to satisfy the reason stated and will ensure the data is validated. The individual will be informed of any decisions made, and where possible, be involved.

J) DATA SECURITY

All Mind in Kingston's staff are aware that hard copies (i.e. paper copies) of personal information should be kept in a locked filing cabinet, drawer, or safe.

Staff are aware of their roles and responsibilities when their role involves the processing of data. All staff are instructed to store files or written information of a confidential nature in a secure manner so that they are only accessed by people who have a need and a right to access them. All staff will ensure that screen locks are implemented on all PCs, laptops, work phones and other devices when they their desk in the office. Where staff use devices outside of the office, devices will be kept with staff at all times and kept locked when not in use.

No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media such as a USB stick, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Staff must always use the passwords provided to access the computer system and not pass them on to people who should not have them.

Personal data relating to relevant individuals should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:

a) ensuring that data is recorded on such devices only where absolutely necessary.
b) using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
c) ensuring that laptops or USB drives are not left where they can be stolen.

Failure to follow Mind in Kingston's rules on data security may be dealt with via Mind in Kingston's disciplinary procedure. This can result in dismissal with or without notice dependent on the severity of the failure.

K) THIRD PARTY PROCESSING

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain Mind in Kingston's commitment to protecting data.

L) INTERNATIONAL DATA TRANSFERS

Mind in Kingston does not transfer personal data to any recipients outside of the EEA.

M) REQUIREMENT TO NOTIFY BREACHES

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

More information on breach notification is available in our Breach Notification policy.

N) TRAINING

New staff must read the policies and procedures on data protection as part of their induction, and will be asked to sign a form to confirm they understand how to use and apply the GDPR policy and procedures.

All staff receive training covering confidentiality, data protection, collecting and storing data and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for Mind in Kingston are trained appropriately in their roles under the GDPR.

All staff who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and Mind in Kingston of any potential lapses and breaches of Mind in Kingston's policies and procedures.

O) RECORDS

Mind in Kingston keeps records of its processing activities including the purpose for the processing and retention periods in its HR Data Record. These records will be kept up to date so that they reflect current processing activities.

P) DATA PROTECTION COMPLIANCE

Our Data Protection Officer is:

Chief Executive Officer
Mind in Kingston
Siddeley House
50 Canbury Park Road
Kingston upon Thames
KT2 6LX

Version No	Author	Purpose/ change	Date
01	Peninsula (HRSC)	To adopt new policy following introduction of GDPR	Jan 2018
02	RE (HRSC)	Update/ review	April 2019
02	RE (HRSC)	Update/ review	November 2021