

## PRIVACY AND DATA PROTECTION POLICY (GDPR)

### Privacy Policy And Data Protection Policy (GDPR)

**Who is responsible: GDPR lead, all managers, all staff, volunteers**

**People involved:** service users, all staff, trustees, volunteers, visitors, , funders, donors, partners, suppliers

**Document Number: 6**

**Status: Live Document**

**Reviewed by** Sigal Avni

**Date:** November 2025 - April 2026

**Date of next review: April 2027**

**Ratified:** Gwen Williams (Chair of the Trustees)

**Replaces document: November 2023**

#### **Summary of main changes since last review:**

1. updated responsibilities including DPO contact

Added:

2. ICO number included

3. lawful basis matrix (processing activity → legal basis)

4. Added to B. DPIA

5. Subject Access Request (SAR) procedure & timelines (one month; ID requirements; how to submit)

6. Retention schedule / table with specific retention periods for categories of data.

7. Third-party processors register

8. Data Breach / Incident response summary

9. children & young people's data / safeguarding & parental consent

10. Cookies / website tracking & analytics + opt-out.

11. Automated decision-making / profiling details & DPIA

12. Records of Processing Activities (RoPA) and accountability statements

#### **CONTENT:**

**A. INTRODUCTION, SCOPE AND RESPONSIBILITIES**

**B. HOW WE COLLECT INFORMATION AND DATA PROTECTION ASSESMENT (DPIA)**

**C. THE INFORMATION WE COLLECT AND WHY WE USE IT**

**D. MARKETTING**

**E. SHARING INFORMATION / PERSONAL DATA**  
**F. KEEPING AND STORING INFORMATION**  
**G. YOUR RIGHTS OVER YOUR PERSONAL INFORMATION**  
**H. MOTINIGING AND DATA PROTECTION**  
**I. OTHER MIND POLICIES**

**Appendix 1 – General Privacy Notice**

**Appendix 2 - Consent Form for Service Users and Volunteers**

**Appendix 3 – Privacy Notice Job Applicant**

**Appendix 4 – Privacy Notice Employee**

## **A. INTRODUCTION, SCOPE AND RESPOSIBILITIES**

This Privacy Policy explains how Islington Mind collects, uses, stores and disposes of personal information, meaning any information that identifies or could identify an individual. It sets out how we comply with the UK GDPR and the Data Protection Act 2018, and provides a framework for ensuring that personal data is handled lawfully, fairly, securely and transparently.

At Islington Mind, we are committed to protecting the personal information of service users, employees and volunteers, and to ensuring that all personal data is processed in a fair, open and transparent manner.

The key data protection principles we follow are that personal data must be:

- lawful, fair and transparent;
- collected for specific purposes;
- adequate, relevant and limited to what is necessary;
- accurate and kept up to date;
- retained only as long as necessary; and
- processed securely.

Islington Mind is registered with the Information Commissioner's Office (ICO) as a data controller (Registration number: ZB673659). As the data controller, Islington Mind is responsible for, and controls, the processing of personal information.

### **Scope**

This policy applies to trustees, staff, contractors and volunteers, and covers the personal data of service users, employees, volunteers, donors, funders, suppliers and partners.

## Responsibilities

- **Data Controller:** Sigal Avni
- **Trustees:** Provide oversight and accountability
- **Data Protection Officer (DPO):** Gemma Watts, Head of Services & Quality
- **All managers, staff, contractors and volunteers:** Must comply with this policy

For further information about our privacy practices, please contact our Data Protection Officer (DPO), Gemma Watts, Head of Services and Quality:

- **Post:** Islington Mind, Unit 4, Archway Business Centre, 19-23 Wedmore Street, Islington, London, N19 4RU
- **Phone:** 020 3301 9850
- **Email:** gemma.watts@islingtonmind.org.uk, admin@islingtonmind.org.uk, or info@islingtonmind.org.uk

## B. HOW WE COLLECT INFORMATION AND DATA PROTECTION ASSESSMENT (DPIA)

At Islington Mind, our aim is to support people experiencing mental health challenges with respect and care. To do this effectively, we collect certain personal information so that:

- Service users, volunteers and employees receive communications relevant to them.
- We can provide the right support when people use our services, volunteer, apply for work, or donate to us.

We collect information in the following ways:

### Direct Contact

We collect information when you contact us directly — for example to:

- Ask about our activities or mental health services.
- Register for services, training or events.
- Make a donation.
- Apply for a job or volunteering opportunity.

This may include contact by phone, post, email, in person, or via our website.

**All service users and volunteers are asked to sign a consent form allowing us to store and use their personal information (see Appendix 1).**

### Through Partners Acting on Our Behalf

Sometimes we receive information through trusted partners who deliver services for us — for example, clinical supervision for volunteer counsellors. These partners act strictly under our instruction and with appropriate safeguards.

### Through Third Parties

If you donate to us through a third-party platform (e.g. MyDonate), we may receive your personal information if you give the platform permission to share it with us.

### Website Use

When you visit our website, we collect general information such as:

- Pages you visit most often.
- Services, events or information you show interest in.

We also use cookies and similar technologies.

### Data Protection Impact Assessment (DPIA)

Before introducing a new way of collecting, storing or processing personal data, Islington Mind will complete a Data Protection Impact Assessment (DPIA). This assessment considers whether the processing is necessary, what the potential privacy impact may be, the risks involved, and how those risks can be minimised. The results will be recorded and shared as appropriate.

## C. THE INFORMATION WE COLLECT AND WHY WE USE IT

Collecting accurate information helps us provide the right services, support and communications to each person.

### 2. Types of Information We Collect

Type of Information	Examples	How We Collect It
<b>Personal Information</b>	Name, date of birth, email address, postal address, phone number, payment details (if making a donation or purchase), and other information you provide when registering with our services, making a donation, signing up for an event, or communicating with us.	Directly from you (online forms, phone calls, email, post, in person).
<b>Sensitive / Special Category Data</b>	Racial or ethnic origin, religion or beliefs, physical or mental health conditions, sexuality. This data is treated with extra care and confidentiality.	Directly from you when necessary to provide a service, with your explicit consent (or another lawful basis, e.g. safeguarding).
<b>Children and Young People</b>	Data about under-18s receiving services. We follow safeguarding	Directly from the young person and/or

Type of Information	Examples	How We Collect It
	guidance and seek parental consent where appropriate.	parent/guardian, with additional safeguards.

## Why We Use Personal Information

We use the information you provide us to:

- Plan and deliver services.
- Create person-centred support plans.
- Liaise with other services on your behalf.
- Help protect you or others from abuse or harm.
- Arrange and deliver services and support.
- Ensure our services are accessible to all.
- Meet responsibilities to staff and volunteers, including HR administration.
- Enable regulators and inspectors to check our services meet required standards.
- Review, audit and improve our services.
- Meet funder monitoring requirements.
- Promote our services and fundraising (with consent or legitimate interest).
- Keep records of our work and our relationship with you.
- Process donations or other payments, claim Gift Aid and verify transactions.
- Send administrative updates (e.g. about an event, donation or service).
- Comply with legal requirements to identify and verify supporters who make major gifts.
- Contact agencies about their work and invite people to surveys, research or events (with consent where needed).

Without certain personal information we may not be able to provide services, process donations or register you for events.

## Lawful Basis for Using Your Information

We only process your data where we have a lawful basis under UK data protection law. The table below summarises our most common activities and the lawful basis relied upon:

Processing Activity	Examples	Lawful Basis
<b>Service delivery</b> (case records, health information)	Creating support plans, safeguarding, referring to other services	Legal obligation / legitimate interests / vital interests (for safety)
<b>Employment records</b> (staff and volunteers)	Payroll, tax, HR files, DBS checks	Contract / legal obligation

Processing Activity	Examples	Lawful Basis
<b>Fundraising and marketing</b>	Sending newsletters, appeals, or event invitations	Consent or legitimate interests (always respecting opt-outs)
<b>Donor due diligence &amp; major gifts</b>	Anti-money laundering checks, verifying identity	Legitimate interests / legal obligation
<b>Research and service evaluation</b>	Surveys, monitoring, analysis	Legitimate interests or consent (depending on sensitivity)

**Records of Processing Activities (RoPA) are maintained. The lawful basis for each activity is documented, for example consent, contract, legal obligation, vital interests or legitimate interests.**

## D. MARKETING

We may send information about our work, events and ways to support us by phone, email, text message or post — unless you have asked us not to.

- You can update your choices or opt out at any time by contacting **info@islingtonmind.org.uk**.
- If a service user agrees to share their personal story on our marketing campaigns or website, they can choose to remain anonymous.
- Marketing consent is recorded and managed via our CRM. Where consent is relied upon, we keep an auditable record of the consent given and how it can be withdrawn.

## E. SHARING INFORMATION / PERSONAL DATA

We use personal information primarily to deliver services safely and effectively. We never sell or share service users' personal information for marketing purposes.

### Sharing with Trusted Partners

We may share personal data with trusted partners who work with us or on our behalf to deliver services, process donations, manage communications or support our operations.

Data is only shared with authorised partners. No unauthorised transfer of personal data outside the UK/EEA will take place without appropriate safeguards.

Examples include:

Category of Partner	Purpose
Payment processors / Gift Aid agents	Processing donations and claiming Gift Aid
CRM providers, cloud storage and backup providers	Secure data storage and management
Email, text and social media platforms	Communication with service users and supporters
HR/payroll providers	Managing staff and volunteer records
Professional advisers (legal/audit)	Compliance and auditing
Commissioned service delivery partners	Providing specialist or localised services

All processing by these partners is carried out under our instruction. We ensure they:

- Store data securely and delete it when no longer needed.
- Use data only for the agreed purpose.
- Comply with Data Protection Laws and have appropriate security measures.

A third-party processor register is maintained and is available on request from our DPO.

### Working with Third Parties – Good Practice

When sharing personal data with a third party, our GDPR Officer ensures:

- **Lawfulness, fairness and transparency** in data processing.
- A clear **lawful basis** for sharing (e.g. necessary to provide the service safely and effectively).
- **Consent** from the data subject where required.
- An **Information and Data Sharing Agreement** is in place.

Due diligence checks include:

- Confirming the third party complies with Data Protection laws, including GDPR.
- Reviewing their Privacy/Data Protection/GDPR policies and security certifications.
- Ensuring they do not transfer data to another third party or outside the UK/EEA without safeguards.
- Verifying technical, physical and organisational security measures and breach-reporting procedures.

### International Transfers

If any personal data is transferred outside the UK/EEA, we will only do so where appropriate safeguards are in place (e.g. UK adequacy decisions, standard contractual clauses or other permitted mechanisms). Details are available from our DPO.

### Legal Disclosure

We may disclose personal information where required by law, regulation, or a valid request from a competent authority.

## F. KEEPING AND STORING INFORMATION

### How We Protect Personal Information

We take the security of personal information very seriously. We use a combination of **physical, technical and organisational measures** to protect data under our control — both online and offline — against unauthorised access, use, alteration, destruction or loss.

#### Our security measures include:

- Role-based access controls so only authorised staff can see personal data.
- Encrypted devices and secure cloud storage.
- Strong password policies and multi-factor authentication on key systems.
- Regular system backups.
- Secure disposal of paper and electronic records.
- Mandatory data protection training for all staff (on induction and at regular refreshers).

### Internet and Third-Party Links

Transmission of data over the internet can never be 100% secure. While we do our best to protect information sent to us online, we cannot guarantee its security in transit.

Our websites may contain links to other sites. We aim to link only to organisations that share our high standards, but we are **not responsible for the content or privacy practices of external sites**. These sites may collect personal information independently of us. This privacy notice does not cover their practices.

### Payment Security

Any debit or credit card details received via our website are passed securely to **Sage Pay**, our payment-processing partner, in compliance with **Payment Card Industry Security Standards**.

## Data Retention – Summary

We keep personal information only for as long as necessary to fulfil the relevant purpose, contractual obligation or legal requirement. Our Data Retention Schedule sets out detailed retention periods and is maintained by the Head of Finance & HR (available on request). For more details, please refer to our **Data Retention and Disposal Policy** and our **Records of Processing Activities (RoPA)**.

In summary, typical retention periods are:

Type of Record	Typical Retention Period
Service user records	7 years after case closure (unless otherwise required)
Financial records, donations & Gift Aid	7 years
Employee records	Duration of employment + 6 years post-employment (or longer if required)
Job applicant (unsuccessful)	6–12 months (typically 6 months unless consent is given to retain longer)

### Deleting or Removing Data

- Service user data will be deleted after discharge from services or upon request, subject to legal or contractual requirements.
- If there has been no recorded contact for 7 years, personal data will be removed from our systems.
- The Data Protection Officer (Head of Services & Quality) monitors data retention and review dates.
- If an individual returns to our services after seven years or more, their personal information will need to be collected again.

### Right to Erasure and Exceptions

Individuals have the right to request deletion of their personal data. However, in some cases we are required to retain certain records for longer periods (for example, safeguarding records or statutory obligations). Where deletion is not possible, data will be securely archived and access will be restricted.

## G. YOUR RIGHTS OVER YOUR PERSONAL INFORMATION

You have a number of rights under data protection law. This section explains those rights and how to exercise them.

To exercise any of these rights, please contact:

- **Post:** Islington Mind, Unit 4, Archway Business Centre, 19–23 Wedmore Street, Islington, London N19 4RU
- **Email:** [info@islingtonmind.org.uk](mailto:info@islingtonmind.org.uk)
- **Phone:** 020 3301 9850

You can also complain directly to the **Information Commissioner’s Office (ICO)** – the UK data protection regulator – at <https://ico.org.uk>.

## Making a Subject Access Request (SAR)

- Write to our **DPO** - [gemma.watts@islingtonmind.org.uk](mailto:gemma.watts@islingtonmind.org.uk) or by post at the address above.
- We normally respond within **one calendar month** of receiving your request and ID; complex or multiple requests may take up to **two additional months** (we will tell you if this applies).
- We may need proof of identity (for example, a copy of photo ID and proof of address) before releasing your personal data.

## Your Main Rights

Right	What It Means
<b>Access</b>	You can request a copy of the personal information we hold about you and details of how we use it. Requests are free of charge.
<b>Rectification</b>	You can ask us to correct or complete inaccurate or incomplete personal information.
<b>Erasure (“Right to be Forgotten”)</b>	You can ask us to delete your personal information where it’s no longer needed, you withdraw consent, or we have no lawful basis to keep it.
<b>Restriction</b>	You can ask us to restrict the use of your information (for example while a complaint is being investigated).
<b>Portability</b>	You can ask us to provide some of your data in a structured, electronic format so you can transfer it to another organisation.
<b>Objection</b>	You can object to our processing where we rely on “legitimate interests” and your situation gives you reasons to object.
<b>Consent Withdrawal</b>	If you’ve given consent (e.g. for marketing), you can withdraw it at any time.

We do **not** carry out automated decision-making.

## Limits to These Rights

Some rights only apply in certain circumstances. If we cannot fulfil your request, we will explain why.

## Complaints

If you are unhappy with our response after contacting the DPO, you can raise the matter with the **ICO** at <https://ico.org.uk>.

## H. MONITORING DATA PROTECTION AND TRAINING

### Monitoring Communications

We may record or monitor communications with us - including phone calls and emails — for **training, quality control and compliance**. This helps us improve our service standards and keep accurate records.

### Data Breach Response

We have a **Data Breach Policy and Incident Response Plan**. If a personal data breach occurs:

- We will assess the risk immediately.
- If legally required, we will **notify the ICO within 72 hours**.
- If the breach poses a high risk to individuals' rights and freedoms, we will **inform affected people directly**.
- We record lessons learned and use them to improve our processes.

### Records of Processing and DPIAs

For any **high-risk processing** - for example, new systems, large-scale special category data, or systematic monitoring - we will complete a **Data Protection Impact Assessment (DPIA)** before starting the activity.

All employees are responsible to report all data breaches are reported immediately to the DPO, who will advise on risk assessment, actions and next steps. High-risk breaches will be reported to affected individuals together with mitigating actions, and they will be advised of their right to complain to the ICO.

We keep an up-to-date **RoPA** and DPIAs.

### Training & Audit

All staff and volunteers are required to complete data protection training as part of their induction, including the NHS Data Security and Protection Toolkit e-learning for social care staff (minimum of 4 modules at induction). Additional role-specific training is provided where required.

Data protection training is refreshed regularly to ensure ongoing compliance. The Finance Subcommittee is responsible for reviewing data protection compliance annually.

## **I. OTHER ISLINGTON MIND POLICIES**

This policy should be read in conjunction with other relevant Islington Mind policies, specifically with our Confidentiality Policy, Data Breach Policy, Data Retention and Disposal Policy, Complaints Policy and Procedure, Safeguarding Policy, Information Governance Policy, IT Security Policy, Communication Policy and Homeworking Policy.

## Appendix 1 –

### Privacy Statement (Privacy Notice)

#### Who We Are

Islington Mind is a registered charity supporting people with mental health challenges. We are a registered Data Controller with the ICO (Reg. No. ZB673659).

**Data Protection Officer:** Gemma Watts

Address: Unit 4, Archway Business Centre, 19–23 Wedmore Street, Islington, London, N19 4RU

Email: [gemma.watts@islingtonmind.org.uk](mailto:gemma.watts@islingtonmind.org.uk) / [info@islingtonmind.org.uk](mailto:info@islingtonmind.org.uk)

Phone: 020 3301 9850

#### 1. Information We Collect

- Personal information (name, contact, DOB, donations).
- Special category (health, ethnicity, religion).
- Employment/volunteering records.
- Website cookies and analytics.

#### 2. How We Use Your Data

Deliver services. Manage volunteering and employment. Process donations. Contact you about services/events. Monitor services. Meet legal/safeguarding obligations.

#### 3. Lawful Basis for Processing

Contract, consent, legal obligation, legitimate interests, vital interests.

#### 4. Sharing Your Information

Never sold. Shared only with IT/cloud providers, HR/payroll, professional advisers, funders, regulators, and service partners. Safeguards for international transfers.

#### 5. How We Protect Your Data

Encryption, access controls, secure disposal, staff training, secure payment processing.

#### 6. How Long We Keep Data

Service user: 7 years post-closure. Financial/donations: 7 years. Employees: 6 years post-employment. Job applicants: 6–12 months.

#### 7. Your Rights

Access, correction, erasure, restriction, portability, objection, withdraw consent, complain to ICO.

#### 8. Cookies & Online Tracking

We use cookies to analyse traffic and improve services. You can disable cookies in your browser.



**Appendix 2:****Consent to keep information about you****Who we are**

Here at Islington Mind, we are committed to protecting your personal information and making every effort to ensure that your personal information is processed in a fair, open and transparent manner.

**Why we want to use your data**

- In order to provide the services you have requested, we might share your information with external organisations or agencies to aid the delivery of that particular service.
- To update you with important administrative messages about the services you have requested.
- To keep a record of your relationship with us.
- Where you volunteer with us, to administer the volunteering arrangement.
- Where you are a client accessing our services, to ensure we provide you with the best services and to meet the needs of our funders' monitoring procedures.
- To contact you about our work and how you can support Islington Mind.
- To invite you to participate in surveys or research.

If we don't have this information, we are very limited in the services and support that we are able to provide.

**The type of data that will be collected and used**

Personal information we collect includes details such as your name, date of birth, email address, postal address, telephone number and credit/debit card details (if you are making a purchase or donation), as well as information you provide in any communications between us. You will have given us this information whilst making a donation, registering for an event, placing an order on our website or any of the other ways you interact with us.

We may carry out automated profiling, but we do not currently carry out solely automated decision-making that has legal or similarly significant effects on you. We will not be transferring your data outside the EEA

**Your right to withdraw consent**

If you have given us your consent to use personal information (for example, for marketing), you can withdraw your consent at any time.

Name.....  
Signature.....  
Date.....

### Appendix 3 – Privacy Notice For Job Applicant

#### Privacy Notice for Job Applicants

In accordance with the General Data Protection Regulation (GDPR), we have implemented this privacy notice to inform you, as prospective employees of our Company, of the types of data we process about you.

We also include within this notice the reasons for processing your data, the lawful basis that permits us to process it, how long we keep your data for and your rights regarding your data.

#### A) 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 is fair, lawful and transparent
- b) data is collected for specific, explicit, and legitimate purposes
- c) data collected is adequate, relevant and limited to what is necessary for the purposes of processing
- d) data is 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 is 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 comply with the relevant GDPR procedures for international transferring of personal data

#### B) TYPES OF DATA HELD

We keep several categories of personal data on our prospective employees in order to carry out effective and efficient processes. We keep this data in recruitment files relating to each vacancy and we also hold the data within our computer systems, for example, recruitment logs. Specifically, we hold the following types of data:

- a) personal details such as name, address, phone numbers;

- b) name and contact details of your next of kin;
- c) your photograph;
- d) your gender, marital status, information of any disability you have or other medical information;
- e) right to work documentation;
- f) information on your race and religion for equality monitoring purposes;
- g) information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter;
- h) references from former employers;
- i) details on your education and employment history etc;
- j) driving licence;
- k) criminal convictions.

## **C) COLLECTING YOUR DATA**

You provide several pieces of data to us directly during the recruitment exercise.

In some cases, we will collect data about you from third parties, such as employment agencies, former employers when gathering references or credit reference agencies.

Should you be successful in your job application, we will gather further information from you, for example, your bank details and next of kin details, once your employment begins.

## **D) LAWFUL BASIS FOR PROCESSING**

Article 6(1)(a) – (Consent) and Article 9(2)(b) – (Employment) of the GDPR Act 2018 allow us to process your data for recruitment and employment purposes. Applying for a job with us means you have given us explicit consent to use your data for purposes of providing employment to you. The information below categorises the types of data processing we undertake under this lawful basis.

Activity requiring your data Lawful basis:

Carrying out checks in relation to your right to work in the UK

Making reasonable adjustments for disabled employees

Making recruitment decisions in relation to both initial and subsequent employment e.g. promotion

Making decisions about salary and other benefits

Making decisions about contractual benefits to provide to you

Assessing training needs

Dealing with legal claims made against us

Preventing fraud

## **E) SPECIAL CATEGORIES OF DATA**

Special categories of data are data relating to your:

- a) health
- b) sexual orientation
- c) race
- d) ethnicity
- f) political opinion
- g) religion
- h) trade union membership

## **F) FAILURE TO PROVIDE DATA**

Your failure to provide us with data may mean that we are unable to fulfil our requirements for entering into a contract of employment with you.

This could include being unable to offer you employment, or administer contractual benefits.

## **G) CRIMINAL CONVICTION DATA**

We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. This data will usually be collected at the recruitment stage, however, may also be collected during your employment. We use criminal conviction data to determine your suitability, or your continued suitability for the role. We rely on the lawful basis of a legal obligation to process this data.

## **H) WHO WE SHARE YOUR DATA WITH**

Employees within our company who have responsibility for recruitment will have access to your data which is relevant to their function. All employees with such responsibility have been trained in ensuring data is processing in line with GDPR.

## **I) PROTECTING YOUR DATA**

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such.

## **J) RETENTION PERIODS**

We only keep your data for as long as we need it for, which, in relation to unsuccessful candidates, is six months to a year.

If your application is not successful and we have not sought consent or you have not provided consent upon our request to keep your data for the purpose of future suitable job vacancies, we will keep your data for six months once the recruitment exercise ends.

If we have sought your consent to keep your data on file for future job vacancies, and you have provided consent, we will keep your data for nine months once the recruitment exercise ends. At the end of this period, we will delete or destroy your data, unless you have already withdrawn your consent to our processing of your data in which case it will be deleted or destroyed upon your withdrawal of consent.

Where you have provided consent to our use of your data, you also have the right to withdraw that consent at any time. This means that we will stop processing your data and there will be no consequences of withdrawing consent.

If your application is successful, your data will be kept and transferred to the systems we administer for employees. We have a separate privacy notice for employees, which will be provided to you.

## **K) AUTOMATED DECISION MAKING**

Automated decision making means making decision about you using no human involvement e.g. using computerised filtering equipment. No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

## **L) YOUR 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. We operate a separate Subject Access Request policy and all such requests will be dealt with accordingly;
- 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.

In addition to the above rights, you also have the unrestricted right to withdraw consent, that you have previously provided, to our processing of your data at any time. Withdrawing your consent means that we will stop processing the data that you had previously given us consent to use.

There will be no consequences for withdrawing your consent. However, in some cases, we may continue to use the data where so permitted by having a legitimate reason for doing so.

If you wish to exercise any of the rights explained above, please contact our Data Protection Officer - Gemma Watts - [gemma.watts@islingtonmind.org.uk](mailto:gemma.watts@islingtonmind.org.uk)

## **M) MAKING A COMPLAINT**

If you think your data rights have been breached, you are able to raise a complaint with the Information Commissioner (ICO). You can contact the ICO at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by telephone on 0303 123 1113 (local rate) or 01625 545 745.

## **N) DATA PROTECTION COMPLIANCE**

Our Data Protection Lead is:

Gemma Watts [gemma.watts@islingtonmind.org.uk](mailto:gemma.watts@islingtonmind.org.uk) 020 3301 9850

**Appendix 4 – Privacy Notice Employees****Privacy Notice for Employees**

In accordance with the General Data Protection Regulation (GDPR), we have implemented this privacy notice to inform you, as prospective employees of our Company, of the types of data we process about you.

We also include within this notice the reasons for processing your data, the lawful basis that permits us to process it, how long we keep your data for and your rights regarding your data.

This notice applies to current and former employees and workers.

**A) 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 is fair, lawful and transparent.
- b) data is collected for specific, explicit, and legitimate purposes.
- c) data collected is adequate, relevant and limited to what is necessary for the purposes of processing.
- d) data is 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 is 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 comply with the relevant GDPR procedures for international transferring of personal data.

**B) TYPES OF DATA HELD**

We keep several categories of personal data on our employees in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, for example, our holiday booking system.

Specifically, we hold the following types of data, as appropriate to your status:

- a) personal details such as name, address, phone numbers
- b) name and contact details of your next of kin.
- c) your photograph
- d) your gender, marital status, information of any disability you have or other medical information.
- e) right to work documentation
- f) information on your race and religion for equality monitoring purposes
- g) information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter.
- h) references from former employers
- i) details on your education and employment history etc
- j) National Insurance numbers
- k) bank account details
- l) tax codes
- m) driving licence
- n) criminal convictions
- o) 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.
  - vi) information on time off from work including sickness absence, family related leave etc.
- p) CCTV footage
- q) building access card records
- r) IT equipment use including telephones and internet access.

## **C) COLLECTING YOUR DATA**

You provide several pieces of data to us directly during the recruitment period and subsequently upon the start of your employment.

In some cases, we will collect data about you from third parties, such as employment agencies, former employers when gathering references or credit reference agencies.

Personal data is kept in files or within the Company's HR and IT systems.

## **D) LAWFUL BASIS FOR PROCESSING**

The law on data protection allows us to process your data for certain reasons only. We process your data in order to comply with a legal requirement or in order to effectively manage the employment contract we have with you, including ensuring you are paid correctly.

The information below categorises the types of data processing, appropriate to your status, we undertake and the lawful basis we rely on.

Activity requiring your data	Lawful basis
Carry out the employment contract that we have entered into with you e.g., using your name, contact details, education history, information on any disciplinary, grievance procedures involving you	Consent and contract of employment
Ensuring you are paid	Contract of Employment
Ensuring tax and National Insurance is paid	Legal obligation
Carrying out checks in relation to your right to work in the UK	Legal obligation
Making reasonable adjustments for disabled employees	Legal obligation
Making recruitment decisions in relation to both initial and subsequent employment e.g., promotion	Legitimate interest
Making decisions about salary and other benefits	Legitimate interest
Ensuring efficient administration of contractual benefits to you	Contract of employment and legitimate interest
Effectively monitoring both your conduct, including timekeeping and attendance, and your performance and to undertake procedures where necessary	Legitimate interest
Maintaining comprehensive up to date personnel records about you to ensure, amongst other things, effective correspondence can be achieved and appropriate contact points in the event of an emergency are maintained	Legitimate interest Legal obligation
Implementing grievance procedures	Legitimate interest
Assessing training needs	Legitimate interest
Implementing an effective sickness absence management system including monitoring the amount of leave and	Legitimate interest

subsequent actions to be taken including the making of reasonable adjustments	
Gaining expert medical opinion when making decisions about your fitness for work	Legitimate interest
Managing statutory leave and pay systems such as maternity leave and pay etc	Legitimate interest
Business planning and restructuring exercises	Legitimate interest
Dealing with legal claims made against us	Legitimate interest
Preventing fraud	Legitimate interest
Ensuring our administrative and IT systems are secure and robust against unauthorised access	Legitimate interest
Providing employment references to prospective employers, when our name has been put forward by the employee/ex-employee, to assist with their effective recruitment decisions	Legitimate interest of the prospective employer

**E) SPECIAL CATEGORIES OF DATA**

Special categories of data relating to your:

- a) health
- b) sexual orientation
- c) race
- d) ethnic origin
- e) political opinion
- f) religion
- g) trade union membership
- h) biometric data.

We carry out processing activities using special category data:

- a) for the purposes of equal opportunities monitoring
- b) in our sickness absence management procedures
- c) to determine reasonable adjustments

Most commonly, we will process special categories of data when the following applies:

- a) you have given explicit consent to the processing
- b) we must process the data in order to carry out our legal obligations
- c) we must process data for reasons of substantial public interest

d) you have already made the data public.

#### **i) FAILURE TO PROVIDE DATA**

Your failure to provide us with data may mean that we are unable to fulfil our requirements for entering into a contract of employment with you. This could include being unable to offer you employment or administer contractual benefits.

#### **j) CRIMINAL CONVICTION DATA**

We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. This data will usually be collected at the recruitment stage, however, may also be collected during your employment.

We use criminal conviction data to determine your suitability, or your continued suitability for the role. We rely on the lawful basis of a legal obligation to process this data.

#### **k) WHO WE SHARE YOUR DATA WITH**

Employees within our company who have responsibility for recruitment, administration of payment and contractual benefits and the carrying out performance related procedures will have access to your data which is relevant to their function. All employees with such responsibility have been trained in ensuring data is processed in line with GDPR.

#### **l) PROTECTING YOUR DATA**

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such through Multi Factor Authentication for access and authorisation process.

#### **m) RETENTION PERIODS**

We only keep your data for as long as we need it for, which will be at least for the duration of your employment with us though in some cases we will keep your data for a period after your employment has ended. Some data retention periods are set by the law. We retain your data for the duration of your employment with us, and 6 years post-employment on lawful basis of legal obligation.

#### **n) AUTOMATED DECISION MAKING**

Automated decision-making means making decision about you using no human involvement e.g., using computerised filtering equipment. No decision will be made about you solely based on automated decision making (where a decision is

taken about you using an electronic system without human involvement) which has a significant impact on you.

## **o) EMPLOYEE RIGHTS**

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

- a. the right to be informed about the data we hold about you and what we do with it;
- b. the right of access to the data we hold about you. More information on this can be found in our separate policy on Subject Access Requests;
- c. the right for any inaccuracies in the data we hold about 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 about 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 employee rights under GDPR.

## **p) CONSENT**

Where you have provided consent to our use of your data, you also have the right to withdraw that consent at any time. This means that we will stop processing your data.

## **q) MAKING A COMPLAINT**

If you think your data rights have been breached, you are able to raise a complaint with the Information Commissioner (ICO). You can contact the ICO at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by telephone on 0303 123 1113 (local rate) or 01625 545 745.

## **r) DATA PROTECTION COMPLIANCE**

Our Data Protection Lead is:

Gemma Watts [gemma.watts@islingtonmind.org.uk](mailto:gemma.watts@islingtonmind.org.uk) 020 3301 9850

Islington Mind's work aims to ensure that we can help people experiencing mental health challenges get support and respect. We want to make sure that our service users and employees receive the communications that are relevant to them through visiting our website or receiving emails, post or phone calls. We want to make sure that people receive the best attention when they become a user of our services, access a volunteering placement or employment opportunity or make a donation.