

## PRIVACY AND DATA PROTECTION POLICY (GDPR)

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

**Who is responsible:** GDPR lead, Head of HR, Finance and Resources all managers, all staff, volunteers

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

**Document Number:** 5

**Status:**

**Reviewed by** Sigal Avni

**Date:** 07/11/2023

**Date of next review:** November 2025

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

**Replaces document:** July 2023

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

1. updated data protection lead to Gerry Turley – Head of Finance, HR and Resources
2. Review of privacy notice for job applicants
3. Review of privacy notice for employees

### CONTENT:

**A. INTRODUCTION**

**B. HOW WE COLLECT INFORMATION**

**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**

**H. MOTINIGING**

**I. OTHER MIND POLICIES**

**Appendix 1 – Consent Form for Service Users and Volunteers**

**Appendix 2 – Privacy Notice Job Applicant**

**Appendix 3 – Privacy Notice Employee**

### A. INTRODUCTION

This Privacy Policy sets out how we collect, use and store your personal information (this means any information that identifies or could identify you).

At Islington Mind, we are committed to protecting service users, employees and volunteer's personal information and making every effort to ensure that personal information is processed in a fair, open and transparent manner.

We are a "data controller" for the purposes of the Data Protection Act 1998 and (from May 2018) the EU General Data Protection Regulation 2016/679 ("Data Protection Law"). This means that we are responsible for, and control the processing of, your personal information.

For further information about our privacy practices, please contact our Data Protection Lead – currently Gerry Turley (Head of Finance, HR and Resources) by:

- Writing to Islington Mind, Unit 4, Archway Business Centre, 19-23 Wedmore Street, Islington, London, N19 4RU
- Calling us on 020 3301 9850
- Emailing to: [Gerry.Turley@islingtonmind.org.uk](mailto:Gerry.Turley@islingtonmind.org.uk) or [admin@islingtonmind.org.uk](mailto:admin@islingtonmind.org.uk) or [min.wilkinson@islingtonmind.org.uk](mailto:min.wilkinson@islingtonmind.org.uk)

**This policy should be read in conjunction with other Islington Mind policies, specifically with our Confidentiality policy, Data Breach Policy and Procedures and Information Governance Policy.**

## B. HOW WE COLLECT INFORMATION

Islington Mind's work aims to ensure that we can help people experiencing mental health problems get both support and respect. We want to make sure that our service users and employees receive the communications that are most relevant to them, be it 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.

We collect information in the following ways:

### B.1 When people interact with us directly:

This could be if people ask us about our activities, register with us for services, training or an event, make a donation to us, ask a question about mental health,

apply for a job or volunteering opportunity or otherwise provide us with personal information. This includes when people phone us, visit our website, or get in touch through the post, or in person.

We ask every service user, and every volunteer to sign a consent form to keep their personal information (see Appendix 1)

## **B.2 When you interact with us through partners on their behalf:**

This could be through being eligible for clinical supervision as a volunteer counsellor which is delivered through trusted individuals working on our behalf and always under our instruction.

## **B.3 When people interact with us through third parties:**

This could be people who provide a donation through a third party such as MyDonate or one of the other third parties that we work with and provide your consent for your personal information to be shared with us.

## **B.4 When you visit our website:**

We gather general information which might include which pages you visit most often and which services, events or information is of most interest to you.

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

The information we collect is used to achieve our vision that everyone experiencing a Mental Health problem gets support and respect.

### **C.1 Personal information**

We collect personal details such as name, date of birth, email address, postal address, telephone number, credit/debit card details (if you are making a purchase or donation), as well as other information provided in any communications with us.

This information is provided to us whilst an individual is registering with our services, making a donation, registering for an event, placing an order on our website or any of the other ways to interact with us.

### **C.2 Sensitive Personal Information**

Certain information is classified as Special Category Data or Sensitive Personal Information. For example, racial or ethnic origin, religious or other beliefs of a

similar nature, physical or mental health conditions and sexuality. This is classed as special because of its sensitive nature.

Sensitive Personal Information will be treated with extra care and confidentiality and always in accordance with this Privacy Policy.

### **C.3 Why Do We Use Personal Information**

We will use the information you provide us with to carry out our work, which will include, amongst others, the following purposes:

- To plan and deliver services.
- To create an appropriate person-centred support plan in line with your needs.
- To liaise effectively with other services for your benefit.
- To help protect you or others from abuse or harm.
- To help you arrange and receive services when needed.
- To ensure our services are accessible to all parts of society.
- To carry out our responsibilities to staff and volunteers, and to administer, and volunteering and employment arrangements.
- So that external regulators and inspectors can check and audit our services and ensure they meet the required standards.
- So that we may review, audit and improve the quality of our services and increase their benefit to you and others.
- To meet the needs of our funders' monitoring procedures.
- To facilitate promotion of our services and fundraising.
- To keep a record of our work and people / companies' relationships with us.
- To process donations or other payments, to claim Gift Aid on donations and verify any financial transactions.
- To update with important administrative messages e.g. about donation, an event or services or goods requested.
- To comply with the Charities (Protection and Social Investment) Act 2016 and follow the recommendations of the official regulator of charities, the Charity Commission, which require us to identify and verify the identity of supporters who make major gifts so we can assess any risks associated with accepting their donations.

#### **We may also use personal information:**

- To contact agencies about their work and how they can support Islington Mind (see D. Marketing' below).
- To invite people to participate in surveys or research or events.

We will not be able to provide services, process donation, sign people up for a particular event without collecting relevant personal information that allows us to provide the requested service or follow up the requested activity.

## C.4 Legal basis for using your information

In some cases, we will only use personal information where we have people's consent to do so or because we need to use it in order to fulfil an agreement or contract. However, there are other lawful reasons that allow us to process personal information and one of those is called 'legitimate interests'. This means that the reason that we are processing information is because there is a legitimate interest for Islington Mind to process personal information to help us to achieve our vision mentioned above.

Whenever we process individual's Personal Information under the 'legitimate interest' lawful basis we make sure that we take into account the individual's rights and interests and will not process personal information if we feel that there is an imbalance.

Some examples of where we have a legitimate interest to process Personal information include where we contact you via post, phone or email, use personal information for data analytics, conducting research to better understand who our supporters are, improving our services, for our legal purposes (for example, dealing with complaints and claims), or for complying with guidance from the Charity Commission.

## D. MARKETTING

We may send information about our work and how to support us and about events by phone, email, text message, and postal address, unless we have been told not to do so or not to do so in that way.

You can update your choices or stop us sending you these communications at any time by contacting [admin@islingtonmind.org.uk](mailto:admin@islingtonmind.org.uk)

If a service user is happy to share personal details with staff members or if they would like us to share their story with the media or other parties as part of our work telling people's personal stories about mental health (for example, on our blog) – they can of course decide if they want to remain anonymous.

## E. SHARING INFORMATION / PERSONAL DATA

The personal information we collect about service users will mainly be used by our staff and volunteers at Islington Mind so that they can provide adequate support. We will never sell or share service users' personal information with organisations for marketing activities.

Islington Mind may however share information with our trusted partners who work with us or on our behalf to deliver our services when sharing of data is required to safely or effectively provide the service. The processing of this information is always carried out under our instruction. We make sure that these partners store the data securely, delete it when they no longer need it and never use it for any other purposes.

Some examples of where we may share information are with our partners who help us to process donations and claim Gift Aid and our partners who help us to manage our social media accounts. When we enter into contracts with these service providers, we require them to comply with Data Protection Laws and ensure that they have appropriate controls in place to secure your information.

## **When Working in Partnership With A Third Party Organisation**

To ensure good and safe practice when sharing personal data with a third-party organisation, the GDPR officer is responsible to ensure:

- compliance with data processing principles (lawfulness, fairness and transparency).
- we also establish a lawful basis for sharing the data (e.g. that sharing of data is required in order to provide the service safely and effectively.)
- that the data subject is aware and consent to the data sharing
- that we document the data sharing through an Information and Data sharing agreement.

The GDPR officer is responsible to ensure that the following due diligence checks of the third party are carried out:

- asking the third-party organisation to confirm they comply with data protection laws, including the General Data Protection Regulation;
- asking the third-party organisation to forward their Privacy / Data Protection / GDPR policies and procedures, and their data security standards certifications, and to confirm that they carry out personal data processing in accordance with their policies and procedures.
- clarifying with the third-party organisation that they do not further transfer personal data to another third party and/or transfer the personal data outside of the European Economic Area;
- establishing with the third-party organisation that they have the technical, physical and organisational security measures in place to protect the personal data. In case of data breach, what is the procedure or

recording pathway from the Organisation Management to the data subject.

## Legal Disclosure

We may disclose information if required to do so by law (for example, to comply with applicable laws, regulations and codes of practice or in response to a valid request from a competent authority.)

## F. KEEPING AND STORING INFORMATION

We take looking after personal information very seriously. We have implemented appropriate physical, technical and organisational measures to protect the personal information we have under our control, both on and off-line, from improper access, use, alteration, destruction and loss.

Unfortunately, the transmission of information using the internet is not completely secure. Although we do our best to protect people's personal information sent to us this way, we cannot guarantee the security of data transmitted to our site. Our websites may contain links to other sites. While we try to link only to sites that share our high standards and respect for privacy, we are not responsible for the content or the privacy practices employed by other sites.

Please be aware that websites that have links on our site may collect personally identifiable information about you. This privacy statement does not cover the information practices of those websites.

Any debit or credit card details which we receive on our website are passed securely to Sage Pay our payment processing partner, according to the Payment Card Industry Security Standards.

### How long we hold your information for

We keep personal information only for as long as is reasonable and necessary for the relevant activity, which may be to provide mental health support services or fulfil statutory obligations (for example, the collection of Gift Aid).

We will delete information from our records, following a service user's discharge from our services, and on their request.

### Removing the information we hold on you

If there has been no recorded contact with you for 7 years or more, we will remove all your data from our systems.

It is the responsibility of our Head of Finance and HR to regularly monitor our systems to check the date of data. S/he will then forward and data to be deleted to our Head of Service and Quality who will approve the deletion.

This will mean if you are referred or self-referred to our services again after a seven year or more period we will need to ask you for your personal information again.

## G. YOUR RIGHTS

You have various rights in respect of the personal information Islington Mind holds about you – these are set out in more detail below. If you wish to exercise any of these rights, you can do so by contacting us at Islington Mind, unit 4, Archway Business Centre, 19-23 Wedmore Street, Islington, London, N19 4RU, by email at [admin@islingtonmind.org.uk](mailto:admin@islingtonmind.org.uk) or by phone on 020 3301 9850.

You can also make a complaint to the data protection supervisory authority, the Information Commissioner's Office, <https://ico.org.uk/>.

### **Access to your personal information**

You have the right to request access to a copy of the personal information that we hold about you, along with information on what personal information we use. You can make this request for access free of charge. Please make all requests for access in writing and provide us with evidence of your identity.

### **Right to object**

You can object to our processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. Please contact us as noted above, providing details of your objection.

### **Consent**

If you have given us your consent to use personal information for other than legal or duty of care reasons, for example, for marketing, you can withdraw your consent at any time.

### **Rectification**

Reviewed: July 2023

Date of next review: July 2025

Page 8 of 22



You can ask us to change or complete any inaccurate or incomplete personal information held about you.

### **Erasure**

You can ask us to delete your personal information where it is no longer necessary for us to use it, you have withdrawn consent, or where we have no lawful basis for keeping it.

### **Portability**

You can ask us to provide you or a third party with some of the personal information that we hold about you in a structured, commonly used, electronic form, so it can be easily transferred.

### **Restriction**

You can ask us to restrict the personal information we use about you where you have asked for it to be erased or where you have objected to our use of it.

We do not currently carry out any automated decision making. Please note, some of these rights only apply in certain circumstances and we may not be able to fulfil every request.

## **H. MONITORING**

We may record your communications with us (including by telephone or email) for training, quality control and compliance purposes to ensure that we continuously improve our customer service standards.

## **I. OTHER POLICIES**

This policy should be read in conjunction with other relevant Islington Mind policies e.g. Confidentiality Policy, Complaints Policy and Procedure, Safeguarding Policy, Information Governance Policy, IT Security Policy, Communication Policy and Homeworking Policy.

## Appendix 1:

### 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 2 – 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 Lead, Gerry Turley  
gerry.turley@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:  
Gerry Turley [gerry.turley@islingtonmind.org.uk](mailto:gerry.turley@islingtonmind.org.uk) 020 3301 9850

## **Appendix 3 – 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.

<b>Activity requiring your data</b>	<b>Lawful basis</b>
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 subsequent actions to be taken including the making of reasonable adjustments	Legitimate interest
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:

Gerry Turley [gerry.turley@islingtonmind.org.uk](mailto:gerry.turley@islingtonmind.org.uk) 020 3301 9850