

Page 1 of 13	<b>DATA PROTECTION POLICY</b>		 <b>Hull and East Yorkshire</b>
Applies to: All paid staff and volunteers			
Prepared by: Justin White/Robin Pillar	Date approved by the Trustees: 15/01/2019	Version 1	<b>Issue Date:</b>

## Section A - What is the policy for?

### 1. Policy statement

Hull and East Yorkshire Mind (the Charity) is committed to protecting personal data and respecting the rights of our **data subjects**; the people whose **personal data** we collect and use. We value the personal information entrusted to us and we respect that trust, by complying with all relevant laws and the General Data Protection Regulation (GDPR) for those who have day-to-day responsibility for data protection and by adopting good practice.

We process personal data to help us:

- a. maintain our list of people using our services;
- b. maintain our list of people who donate money to fund our work;
- c. share anonymised information with donors and potential donors about our work;
- d. provide support for people using our services;
- e. maintain information about partner Charities;
- f. safeguard children, young people and adults at risk;
- g. recruit, support and manage staff and volunteers;
- h. undertake research;
- i. maintain our accounts and records;
- j. promote our activities and services;
- k. maintain the security of property and premises;
- l. respond effectively to enquirers and handle any complaints.

This policy applies to all personal information, whether it is held on paper, digital or other media and has been approved by Hull and East Yorkshire Mind's Trustees, who are responsible for ensuring that we comply with all our legal obligations. It sets out the legal rules that apply whenever we obtain, store or use personal data.

### 2. Why this policy is important

We are committed to protecting personal data from being misused, getting into the wrong hands as a result of poor security or being shared carelessly, or being inaccurate, as we are aware that people can be upset or harmed if any of these things happen.

This policy sets out the measures we are committed to taking as a Charity and, what each of us will do to ensure we comply with the relevant legislation.

In particular, we will make sure that all **personal data** is:

- a. processed **lawfully, fairly and in a transparent manner** in relation to individuals;

- b. collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes;
- c. **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;
- d. **accurate** and, where necessary, kept up to date, taking reasonable steps to erase or rectify inaccurate data without delay;
- e. kept in a form which permits identification of the data subjects for **no longer than is necessary**; and
- f. processed in a manner that ensures **security** of the personal data using appropriate technical and organisational measures.

### 3. How this policy applies to you and what you need to know

**As an employee, trustee or volunteer** processing personal information on behalf of the Charity, you are required to comply with this policy. If you think that you have accidentally breached the policy it is important that you contact a member of the Senior Management Team immediately so that we can take swift action to try and limit the impact of the breach.

Anyone who breaches the Data Protection Policy may be subject to disciplinary action, and where that individual has breached the policy intentionally, recklessly, or for personal benefit they may also be liable to prosecution or to regulatory action.

**As a manager:** You are required to make sure that any procedures that involve personal data, that you are responsible for in your area, follow the rules set out in this Data Protection Policy.

**As a data subject of Hull and East Yorkshire Mind:** We will handle your personal information in line with this policy.

**As an appointed data processor/contractor:** Companies who are appointed by us as a data processor are required to comply with this policy under the contract with us. Any breach of the policy will be taken seriously and could lead to us taking contract enforcement action against the company, or terminating the contract. Data processors have direct obligations under the GDPR, primarily to only process data on instructions from the controller (us) and to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved.

**Our Senior Management Team** is responsible for advising Hull and East Yorkshire Mind and its staff and members about their legal obligations under data protection law, monitoring compliance with data protection law, dealing with data security breaches and with the development of this policy. Any questions about this policy or any concerns that the policy has not been followed should be referred to them at [info@heymind.org.uk](mailto:info@heymind.org.uk) with subject header of "Data Protection – for attention of SMT".

Before you collect or handle any personal data as part of your work (paid or otherwise) for Hull and East Yorkshire Mind, it is important that you take the time to read this policy carefully and understand what is required of you, as well as the Charity's responsibilities when we process data.

Our procedures will be in line with the requirements of this policy, but if you are unsure about whether anything you plan to do, or are currently doing, might breach this policy you must first speak to a member of the Senior Management Team.

## 4. Training and guidance

We will provide annual mandatory online training for all staff to raise awareness of their obligations and our responsibilities, as well as to outline any legislation updates. We may also issue procedures, guidance or instructions from time to time. Managers must set aside time for their team to look together at the implications for their work.

## Section B - Our data protection responsibilities

### 5. What personal information do we process?

In the course of our work, we may collect and process information (personal data) about many different people (data subjects). This includes data we receive straight from the person it is about, for example, where they complete forms or contact us. We may also receive information about data subjects from other sources including, for example, previous employers or other referral services.

We process personal data in both electronic and paper form and all this data is protected under data protection law. The personal data we process can include information such as names and contact details, education or employment details, GP details and visual images of people.

In some cases, we hold types of information that are called '**Special category data**'. This is personal data which the GDPR says is more sensitive, and so needs more protection. This personal data can **only** be processed under strict conditions.

'**Special category data**' (as referred to in the GDPR) includes information about a person's: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health (including physical and mental health, and the provision of health care services); sex life; or sexual orientation.

This type of data could create more significant risks to a person's fundamental rights and freedoms, for example, by putting them at risk of unlawful discrimination

We will not hold information relating to criminal proceedings or offences or allegations of offences unless there is a clear lawful basis to process this data, such as where it fulfils one of the substantial public interest conditions in relation to the safeguarding of children and of individuals at risk, or one of the additional conditions relating to criminal convictions set out in either Part 2 or Part 3 of Schedule 1 of the Data Protection Act 2018.

Other data may also be considered 'sensitive' such as bank details, but will not be subject to the same legal protection as the types of data listed above.

### 6. Making sure processing is fair and lawful

Processing of personal data will only be fair and lawful when the purpose for the processing meets a legal basis, as listed below, and when the processing is transparent. This means we will provide people with an explanation of how and why we process their personal data at the point we collect data from them, as well as when we collect data about them from other sources.

#### a. How can we legally use personal data?

Processing of personal data is only lawful if at least one of these legal conditions, as listed in Article 6 of the GDPR, is met:

**Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

**Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

**Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

**Vital interests:** the processing is necessary to protect someone's life.

**Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

**Legitimate interests:** the processing is necessary for legitimate interests pursued by Hull and East Yorkshire Mind or another Charity, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

## b. How can we legally use 'special categories' of data?

Processing of 'special categories' of personal data is only lawful when, in addition to the conditions above, one of the extra conditions, as listed in Article 9 of the GDPR, is met. These conditions include where:

- i. the processing is necessary for **carrying out our obligations under employment and social security and social protection law;**
- ii. the processing is necessary for **safeguarding the vital interests** (in emergency, life or death situations) **of an individual** and the data subject is incapable of giving consent;
- iii. the processing is carried out in the **course of our legitimate activities** and only relates to our members or persons we are in regular contact with in connection with our purposes;
- iv. the processing is necessary for **pursuing legal claims.**
- v. If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their **explicit consent.**

Before deciding which condition should be relied upon, we should refer to the original text of the GDPR as well as any relevant guidance, and seek legal advice as required.

## c. What must we tell individuals before we use their data?

If personal data is collected directly from the individual, we will inform them about; our identity/contact details, the reasons for processing, and the legal bases, explaining our legitimate interests, and explaining, where relevant, the consequences of not providing data needed for a contract or statutory requirement; who we will share the data with; if we plan to send the data outside of the European Union; how long the data will be stored and the data subjects' rights.

This information is commonly referred to as a 'Privacy Notice'. This information will be given at the time when the personal data is collected.

If data is collected from another source, rather than directly from the data subject, we will provide the data subject with the information described in section 6 as well as: the categories of the data concerned; and the source of the data.

This information will be provided to the individual in writing and no later than within **one month** after we receive the data, unless a legal exemption under the GDPR applies. If we use the data to communicate with the data subject, we will at the latest give them this information at the time of the first communication.

If we plan to pass the data onto someone else outside of Hull and East Yorkshire Mind, we will give the data subject this information **before** we pass on the data.

## **7. When we need consent to process data**

Where none of the other legal conditions apply to the processing, and we are required to get consent from the data subject, we will clearly set out what we are asking consent for, including why we are collecting the data and how we plan to use it. Consent will be specific to each process we are requesting consent for and we will only ask for consent when the data subject has a real choice whether or not to provide us with their data.

Consent can however be withdrawn at any time and if withdrawn, the processing will stop. Data subjects will be informed of their right to withdraw consent and it will be as easy to withdraw consent as it is to give consent.

## **8. Processing for specified purposes**

We will only process personal data for the specific purposes explained in our privacy notices (as described in section 5) or for other purposes specifically permitted by law. We will explain those other purposes to data subjects in the way described in section 5, unless there are lawful reasons for not doing so.

## **9. Data will be adequate, relevant and not excessive**

We will only collect and use personal data that is needed for the specific purposes described above (which will normally be explained to the data subjects in privacy notices). We will not collect more than is needed to achieve those purposes. We will not collect any personal data 'just in case' we want to process it later.

## **10. Accurate data**

We will make sure that personal data held is accurate and, where appropriate, kept up to date. The accuracy of personal data will be checked at the point of collection and at appropriate points later on.

## **11. Keeping data and destroying it**

We will not keep personal data longer than is necessary for the purposes that it was collected for. We will comply with any official guidance issued about retention periods for specific records.

Information about how long we will keep records for can be found in our Retention of Records schedules. These can be found at F:/Proformas/Retention of Records.

## **12. Security of personal data**

We will use appropriate measures to keep personal data secure at all points of the processing. Keeping data secure includes protecting it from unauthorised or unlawful processing, or from accidental loss, destruction or damage.

We will implement security measures which provide a level of security which is appropriate to the risks involved in the processing. Measures will include technical and organisational security measures. In assessing what measures are the most appropriate we will take into account the following, and anything else that is relevant:

- the quality of the security measure;
- the costs of implementation;
- the nature, scope, context and purpose of processing;
- the risk (of varying likelihood and severity) to the rights and freedoms of data subjects;
- the risk which could result from a data breach.

Measures may include:

- technical systems security;
- measures to restrict or minimise access to data;
- measures to ensure our systems and data remain available, or can be easily restored in the case of an incident;
- physical security of information and of our premises;
- organisational measures, including policies, procedures, training and audits; AND
- regular testing and evaluating of the effectiveness of security measures.

The need to ensure that information is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All Data Users are responsible for ensuring that:

- any personal information which they come into contact with is kept securely;
- personal information is not disclosed to any unauthorised third party, whether orally or in writing or accidentally or otherwise; and
- any personal information which is sent to another individual (whether internal or external) must be clearly marked as 'Private and Confidential' and sent to a named person.

Data Users who are employees should note that unauthorised disclosure of personal information by an employee will potentially lead to disciplinary action, and may be considered gross misconduct in sufficiently serious or repeated cases.

The following steps should be taken at all times with regards personal information:

**a. Manually Held Personal Information**

- Manual personal information should be kept in lockable storage when not in use (including but not limited to storing information about service users in a locked cabinet);
- Personal information should not be left unattended, such as on desks or tables (including but not limited to within a project);
- Paper records containing personal information must be shredded and securely disposed of where no longer required (including but not limited to handwritten notes/letters which are subsequently typed up); and
- Personal information must not be left in the photocopier, printer or fax machine.

**b. Electronically Held Personal Information**

- Hard copies of personal information should not be taken from the Charity's computer network unless absolutely necessary;

- Unattended ICT equipment should not be accessible to other users (e.g. via computer screens);
- Where personal information is stored on ICT equipment which is physically installed at the Charity's premises, that equipment must be password protected (as must any files containing personal information held on that equipment);
- Personal information should never be copied onto or stored on any portable equipment or device without specific written authorisation from a member of Senior Management Team;
- Where personal information is stored on any portable equipment or device (including but not limited to USB drives, CD-ROMs, DVD-ROMs and laptop computers), such equipment/device must be encrypted (password protection is not sufficient); Electronically stored personal information must be deleted when no longer required (including where stored on CD-ROM or DVD-ROM); and
- Personal information must not sent by email without specific written authorisation from a member of Senior Management Team (as security cannot be guaranteed), and any personal information sent by email must be password-protected and encrypted.

Data Users must not take any personal information with them away from the premises without specific authorisation from their Line Manager. If any personal information is taken off the premises (whether held on paper or on an electronic device), it should be kept with you or in a secure location at all times (e.g. should be kept in a locked car boot during transit and must never be left unattended in a vehicle, even when parked at home) and should not be accessible by friends or family. In the event that any such information is lost or stolen, or you believe it may have been accessed by an unauthorised person or otherwise compromised, you must report it to a member of the Senior Management Team immediately.

### **13. Keeping records of our data processing**

To show how we comply with the law we will keep clear records of our processing activities and of the decisions we make concerning personal data (setting out our reasons for those decisions).

## **Section C - Working with people we process data about (data subjects)**

### **14. Data subjects' rights**

We will process personal data in line with data subjects' rights, including their right to:

- request access to any of their personal data held by us (known as a Subject Access Request);
- ask to have inaccurate personal data changed;
- restrict processing, in certain circumstances;
- object to processing, in certain circumstances, including preventing the use of their data for direct marketing;
- data portability, which means to receive their data, or some of their data, in a format that can be easily used by another person (including the data subject themselves) or Charity;
- not be subject to automated decisions, in certain circumstances; and
- withdraw consent when we are relying on consent to process their data.

If a colleague receives any request from a data subject that relates or could relate to their data protection rights, this will be forwarded to a member of the Senior Management Team immediately.

We will act on all valid requests as soon as possible, and at the latest within **one calendar month**, unless we have reason to, and can lawfully extend the timescale. This can be extended by up to two months in some circumstances. All data subjects' rights are provided free of charge.

Any information provided to data subjects will be concise and transparent, using clear and plain language.

## 15. Direct marketing

We will comply with the rules set out in the GDPR, the Privacy and Electronic Communications Regulations (PECR) and any laws which may amend or replace the regulations around **direct marketing**. This includes, but is not limited to, when we make contact with data subjects by post, email, text message, social media messaging, telephone (both live and recorded calls) and fax.

**Direct marketing** means the communication (by any means) of any advertising or marketing material which is directed, or addressed, to individuals. "Marketing" does not need to be selling anything, or be advertising a commercial product. It includes contact made by Charities to individuals for the purposes of promoting the Charity's aims.

Any direct marketing material that we send will identify Hull and East Yorkshire Mind as the sender and will describe how people can object to receiving similar communications in the future. If a data subject exercises their right to object to direct marketing we will stop the direct marketing as soon as possible.

## Section D – working with other organisations and transferring data

### 16. Sharing information with other organisations

We will only share personal data with other organisations or people when we have a legal basis to do so and if we have informed the data subject about the possibility of the data being shared (in a privacy notice), unless legal exemptions apply to informing data subjects about the sharing. Only authorised and properly instructed staff/Trustees are allowed to share personal data.

We will keep records of information shared with a third party, which will include recording any exemptions which have been applied, and why they have been applied. We will follow the ICO's statutory [\*Data Sharing Code of Practice\*](#) (or any replacement code of practice) when sharing personal data with other data controllers. Legal advice will be sought as required.

### 17. Data processors

Before appointing a contractor who will process personal data on our behalf (a data processor) we will carry out due diligence checks. The checks are to make sure the processor will use appropriate technical and organisational measures to ensure the processing will comply with data protection law, including keeping the data secure, and upholding the rights of data subjects. We will only appoint data processors who can provide us with sufficient guarantees that they will do this.

We will only appoint data processors on the basis of a written contract that will require the processor to comply with all relevant legal requirements. We will continue to monitor the data processing, and compliance with the contract, throughout the duration of the contract.

## 18. Transferring personal data outside the European Union (EU)

Personal data cannot be transferred (or stored) outside of the European Union unless this is permitted by the GDPR. This includes storage on a “cloud” based service where the servers are located outside the EU.

We will only transfer data outside the EU where it is permitted by one of the conditions for non-EU transfers in the GDPR.

## Section E – Managing change and risks

### 19. Data protection impact assessments

When we are planning to carry out any data processing which is likely to result in a high risk we will carry out a Data Protection Impact Assessment (DPIA). These include situations when we process data relating to vulnerable people, trawling of data from public profiles, using new technology, and transferring data outside the EU. Any decision not to conduct a DPIA will be recorded.

We may also conduct a DPIA in other cases when we consider it appropriate to do so. If we are unable to mitigate the identified risks such that a high risk remains we will consult with the ICO.

DPIAs will be conducted in accordance with the ICO’s Code of Practice ‘[Conducting privacy impact assessments](#)’.

### 20. Dealing with data protection breaches

Where staff or volunteers, [or contractors working for us], think that this policy has not been followed, or data might have been breached or lost, this will be reported **immediately** to a member of the Senior Management Team.

We will keep records of personal data breaches, even if we do not report them to the ICO.

We will report all data breaches which are likely to result in a risk to any person, to the ICO. Reports will be made to the ICO within **72 hours** from when someone in the Charity becomes aware of the breach.

In situations where a personal data breach causes a high risk to any person, we will (as well as reporting the breach to the ICO), inform data subjects whose information is affected, without undue delay.

This can include situations where, for example, bank account details are lost or an email containing sensitive information is sent to the wrong recipient. Informing data subjects can enable them to take steps to protect themselves and/or to exercise their rights.

## 21. Use of CCTV

The Charity has installed CCTV systems at its premises in order to protect the integrity of the Charity's property and the security and health and safety of its employees, volunteers, trustees, students, members, service users and other visitors.

In order to maintain a secure and safe environment for its employees, volunteers, trustees, students, members, service users and other visitors the Charity also needs to monitor its property and the working environment generally to ensure that those individuals are carrying out safe working practices. Using CCTV acts as a deterrent to potential trespassers, thieves and vandals and those who choose to breach the Charity's health and safety rules and other procedures.

The Charity has considered alternatives to using CCTV, such as additional regular inspections of its property, but has concluded that such alternatives would be less effective and more costly. In particular, there are situations which will require a rapid response if the risk to an individual's safety is to be minimised. CCTV is the best way for the Charity to achieve this.

The Charity shall display prominent signs at main entrances to sites where CCTV cameras are present unless in exceptional circumstances it is deemed necessary not to do so. Only senior members of staff have routine access to live and recorded images generated by the CCTV systems, although images will be provided to law enforcement authorities where appropriate. The Charity may use recorded images as evidence in misconduct and performance related investigations as well as in disciplinary and court proceedings.

## Schedule 1 – Definitions and useful terms

The following terms are used throughout this policy and have their legal meaning as set out within the GDPR. The GDPR definitions are further explained below:

**Data controller** means any person, company, authority or other body who (or which) determines the means for processing personal data and the purposes for which it is processed. It does not matter if the decisions are made alone or jointly with others.

The data controller is responsible for the personal data which is processed and the way in which it is processed. We are the data controller of data which we process.

**Data processors** include any individuals or organisations, which process personal data on our behalf and on our instructions e.g. an external Charity which provides secure waste disposal for us. This definition will include the data processors' own staff (note that staff of data processors may also be data subjects).

**Data subjects** include **all** living individuals who we hold or otherwise process personal data about. A data subject does not need to be a UK national or resident. All data subjects have legal rights in relation to their personal information. Data subjects that we are likely to hold personal data about include:

- the people we care for and support;
- our employees (and former employees);
- consultants/individuals who are our contractors or employees working for them;
- volunteers;
- tenants;
- trustees;
- complainants;
- supporters;
- enquirers;
- friends and family;
- advisers and representatives of other organisations.

**ICO** means the Information Commissioners Office which is the UK's regulatory body responsible for ensuring that we comply with our legal data protection duties. The ICO produces guidance on how to implement data protection law and can take regulatory action where a breach occurs.

**Personal data** means any information relating to a natural person (living person) who is either identified or is identifiable. A natural person must be an individual and cannot be a company or a public body. Representatives of companies or public bodies would, however, be natural persons.

Personal data is limited to information about living individuals and does not cover deceased people.

Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

**Privacy notice** means the information given to data subjects which explains how we process their data and for what purposes.

**Processing** is very widely defined and includes any activity that involves the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing can also include transferring personal data to third parties, listening to a recorded message (e.g. on voicemail) or viewing personal data on a screen or in a paper document which forms part of a structured filing system. Viewing of clear, moving or stills images of living individuals is also a processing activity.

**Special categories of data** (as identified in the GDPR) includes information about a person's:

- Racial or ethnic origin;
- Political opinions;
- Religious or similar (e.g. philosophical) beliefs;
- Trade union membership;
- Health (including physical and mental health, and the provision of health care services);
- Genetic data;
- Biometric data;
- Sexual life and sexual orientation.

## Schedule 2 – ICO Registration

**Data Controller:** Hull and East Yorkshire Mind

**Registration Number:** ZA033588

**Date Registered:** 24/12/2013

**Registration Expires:** 23/12/2019

**Address:**

Wellington House

108 Beverley Road

Hull

HU3 1YA