# Mind St Helens
# Data Protection Policy

| | | |
|---|---|---|
| Last Editor | *Paul O'Brien – CEO* | *May 2026* |
| Approver | | |
| Stakeholder groups involved | | |

# Contents

# Introduction

## Purposes

**St Helens Mind is** an independent, user focused charity providing quality services to make a positive difference to the wellbeing and mental health of the people in our local area. During its daily operations, **St Helens Mind receives**, processes, and shares data relating to service users, staff, volunteers, trustees, stakeholders, and donors. **St Helens Mind sees** that earning the trust of stakeholders and people using services around data security is a key part of providing effective services.
To ensure it meets its legal and regulatory responsibilities for the use and storage of this data, it is crucial that **St Helens Mind has** a clear and relevant Data Protection Policy, allowing it to comply with UK General Data Protection Regulation (UK GDPR) and the UK Laws that implement it, including the Data Protection Act 2018. Collectively, these laws are referred to as Data Protection Legislation.

The purpose of Data Protection Legislation is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge. This Data Protection Policy is designed to ensure that **St Helens Mind complies** fully with Data Protection Legislation and that personal data is fairly, lawfully, and transparently processed.

## At A Glance

**St Helens Mind is** registered with the ICO to process certain information about staff, volunteers, service users, and trustees to provide the following:

- Provision of Mental Health services
- Fundraising, campaigning, and membership services
- Monitoring, evaluation, and audit of service provision
- Mental Health and Wellbeing Training in the Community and with local organisations

## Scope

Data Protection Legislation applies to all personal data throughout its lifespan, from point of collection to its eventual destruction. Personal data includes any piece of information which enables identification of a living individual, such as name, contact details, and health information. For the purposes of this policy, references to personal data shall include sensitive personal data unless stated otherwise. This includes personal data collected on all individuals who are affiliated with **St Helens Mind,** including staff, volunteers, service users, and trustees.

The format in which the information is held is, in most cases, not relevant. If personal data exists in any form, whether electronic or in a paper-based filing system, it is covered by this policy and Data Protection Legislation.

At **St Helens Mind,** this policy applies to all staff, volunteers, trustees, and third-party contractors working with the organization. Any person working in these roles should familiarize themselves with this policy and **St Helens Mind 's** other information governance policies and comply with their terms when processing personal data on our behalf.

## How does Data Protection affect me in my role at **St Helens Mind?**

**St Helens Mind could** be fined if you use or disclose information about other people without their consent (or other lawful grounds). To help keep personal data secure, you should take particular care when using the internet, e-mail, or talking on mobile or landline telephones. You could be committing an offense if you steal or recklessly misuse personal data.

Special care must be taken with sensitive personal data such as information relating to race, ethnic origins, religious/political beliefs, health data, disabilities, sexual life, genetics, biometrics, or trade union membership. Details of criminal offense or alleged offense must also be handled with special care.

Any breach of Data Protection Legislation or this policy will be dealt with under **St Helens Mind 's** disciplinary policy. It may also be a criminal offense, in which case **St Helens Mind is** obligated to report the matter as soon as possible to the appropriate authorities.

## Definitions

**Personal data**
Personal data is any information relating to an *identified* or *identifiable* natural person (sometimes called a 'data subject').

- 'Identifiable' means the person can either be 1) identified directly from the information or 2) can be identified indirectly from the information in combination with other information.
- Common identifiers include name, an identification number, location data, or an online identifier (e.g., cookies or an IP address).

Information that is not considered personal data includes:

- Data that has been truly 'anonymised.' In other words, all identifiers have been removed.
- Information about a deceased person.
- Information about companies or public authorities.

**Sensitive or 'Special Categories' of Personal data**
The UK GPDR makes a distinction between personal data and sensitive personal data (sometimes called 'special categories of personal data'). Sensitive personal data requires a higher level of protection.

Sensitive personal data can include:

- Race;
- Ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data (where this is used for identification purposes);
- Health data;
- Sex life; or
- Sexual orientation

Personal data can include information relating to criminal convictions and offenses. This also requires a higher level of protection.

**Data Controllers & Processers**
Data controllers are the main decision-makers about the data, including the purposes for collecting the data and how it is processed (e.g., paper vs. electronic processing). If the organisation decides what data to process and why, it is typically considered the data controller. **St Helens Mind is** registered with the ICO as a data controller. In contrast, a data processor only acts on behalf of and at the instructions of the relevant controller.

# Roles and Responsibilities

## Board of Trustees

The Board of Trustees is responsible for reviewing and approving this policy, as well as ensuring **St Helens Mind is** properly resourced to fulfil the obligations of this policy. The Board of Trustees is also responsible for developing a culture of commitment to transparency that informs all the activities of the charity.

The Board of Trustees is responsible for ensuring they receive appropriate training and advise with regards to UK data protection legislation.

## Data Protection Team

Responsibility for compliance with data protection legislation at **St Helens Mind** rests with the Data Protection Team. This team consists of three senior responsible roles, detailed below.

The Senior Information Risk Owner (SIRO) "owns" the data protection risk of **St Helens Mind** and is responsible for making sure that the Data Protection function is fully resourced to meet the needs of the Charity. In this capacity, the SIRO works with the Board of Trustees and wider Data Protection Team to monitor the information security risks of the organisation and ensure there is sufficient budget to manage these risks. CEO is the named SIRO.

The Caldecott Guardian advises on maintaining confidentiality of the service user health and social care data St Helens Mind collects and accesses. The Caldecott Guardian works closely with the SIRO and DPO to ensure that personal information about the service users who access St Helens Mind services is used legally, ethically, and appropriately. John Astley (Trustee) is the Caldecott Guardian for Mind St Helens.

The Data Protection Officer (DPO) ensures that the organisation complies with UK GDPR and other data protection laws, including monitoring internal compliance, staff training, audits, and managing the data protection policies and procedures of the organisation. The DPO advises on and monitors Data Protection Impact Assessments (DPIAs), responds to Data Subject Access Requests (DSARs), and monitors and updates the Data Map. The DPO is the first contact point for the CEO is the Data Protection Officer.

## Managers & Project Leads

All those in managerial or supervisory roles throughout **St Helens Mind are** responsible for developing and encouraging good information handling practices within the organisation.

Managers and project leads are further designated as Information Asset Owners (IAOs) within their respective departments. IAOs are responsible for promoting data protection awareness and compliance with data protection legislation and this policy within their teams. This includes working with the DPO to complete DPIAs, respond to DSARs, and compile the Data Map.

Managers and project leads are also responsible for making sure that all staff and volunteers in their teams have the necessary data protection training and refreshers.

## All Staff, Volunteers, and Trustees

It is the responsibility of all staff, volunteers, and trustees to ensure they understand and act in accordance with this Policy and Data Protection Legislation.

Staff, volunteers, and trustees should also ensure they keep their line managers and/or the DPO informed if they become aware of any proposed changes to the ways in which personal data is being processed by their team, any possible data breaches that occur, or any DSARs that occur.

Any individual found to be acting contrary to this policy may be subject to disciplinary action. This is because any breach of the data protection legislation could result in **St Helens Mind facing** legal action.

All individuals at **St Helens Mind are** responsible for ensuring that any personal data supplied by them or about them is accurate and up to date.

# Policy Statement

## Aims of this Policy

I. To protect the rights and privacy of living individuals who access **St Helens Mind 's** services, work for, or support **St Helens Mind.** To ensure that personal data is not used, stored, or disclosed without such individual's knowledge, and is processed with a lawful basis and in a fair and transparent manner.

II. To ensure that everyone managing and handling personal data at **St Helens Mind understands** that they are contractually responsible for following good data protection practice, are appropriately trained to do so, and are supported in their role as it regards to data protection.

III. To engage in best practice around data protection principles and procedures, so that any staff, volunteers, service users, and trustees working with **St Helens Mind can** feel confident and trusting in our approach to data protection and that **St Helens Mind will** always act in their best interests.

## Data Protection Principles

**St Helens Mind regards** the lawful and correct treatment of personal information as very important to its successful operation and to maintaining confidence between **St Helens Mind and** those with whom it works. To this end, **St Helens Mind fully** endorses and adheres to the '7 Principles of Good Practice' as set out in the UK GDPR.

The principles say the following:

1. **Lawfulness, fairness, and transparency**: Personal data about individuals must be processed lawfully, fairly, and in a transparent manner.
2. **Purpose limitation**: Personal data must be collected and used only for specified, explicit, and legitimate purposes and must not be further used in any manner incompatible with that purpose. If the organisation processes the data further for the following reasons - in the public interest, scientific or historical research purposes, or statistical purposes – this will not be considered incompatible with the initial purposes.
3. **Data minimisation**: Personal data must be adequate, relevant, and limited to what is necessary to fulfil the 'purposes for which it is processed.'
4. **Accuracy**: Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate personal data are rectified or erased without delay.
5. **Storage limitation**: Personal data (that identifies data subjects) must not be kept for longer than is necessary for the original purposes that the personal data are being processed. However, personal data may be stored for longer periods insofar as the personal data will be

processed solely for: Archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes. This storage extension is subject to the appropriate implementation of technical and organisational measures to ensure that the rights and freedoms of individuals are safeguarded.

6. **Integrity and confidentiality (security)**: Personal data must be processed in a manner that ensures appropriate security of the personal data. This includes protection against unauthorised or unlawful processing and/or against accidental loss, destruction, or damage of the data. The organisation must use appropriate technical or organisational measures.
7. **Accountability**: The data controller (**MIND**) is responsible for and must be able to demonstrate compliance with data protection legislation and these principles.

## Data Mapping

There are several teams at **St Helens Mind who** collect and process personal data. To demonstrate commitment to the principles above, **St Helens Mind will** keep a record of what data it holds, why it collects this data, and where it is stored. This will be maintained in the Data Map (sometimes referred to as a 'Record of Processing Activities' or 'Personal Information Register').

**St Helens Mind is** a data controller under data protection legislation. In some contracts, **St Helens Mind works** in partnership with organisations as a joint data controller or processor. Because of this, **St Helens Mind must** ensure that it has a lawful basis for processing personal data. The Data Protection Officer in conjunction with Data Protection Team, where necessary, will determine the lawful basis for processing personal data. **St Helens Mind will** keep a record of the identified legal basis for processing data in the Data Map.

**St Helens Mind 's** Data Map is stored in **One Drive** and is maintained by. The Data Map will be updated annually, or when relevant data collection practices change (e.g., the addition of a service). For reference, the lawful bases for processing personal data can be found in Appendix A.

## Data Protection Impact Assessments (DPIAs)

Personal data must be protected. **St Helens Mind has** a 'data protection by design and default' approach. This means that whenever a new data collection system or process is introduced or changed, data protection must be considered.

Before introducing or significantly changing a personal data collection system or process, a Data Protection Impact Assessment (DPIA) must be completed and approved by the DPO. The ICO provides a DPIA template that should be used at **St Helens Mind.** A copy of this template is stored on One Drive.

## Consent & Privacy Notices

Personal data should not be obtained, held, used, or disclosed unless the individual has given consent or there is another lawful basis that allows us to do so.

**St Helens Mind understands** "consent" to mean that the data subject has been fully informed of the intended processing and has signified (by an affirmative action) their freely given agreement, preferably in writing, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or based on misleading information will not be considered valid. See **St Helens Mind 's** Consent Policy for further information.

All **St Helens Mind services** should display or make available adequate Privacy Notices to clients explaining how **St Helens Mind processes** their information. We must provide Privacy Notices even if

we do not need to ask for consent or are relying on an alternative legal basis for processing personal data.

## Data Sharing with Third Parties & Information Sharing Agreements (ISAs)

**St Helens Mind must** ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the police. All staff should exercise caution when asked to disclose personal data held on another individual to a third party. All third-party requests to provide data must be supported by appropriate paperwork and specifically authorised by the DPO.

There are restrictions on the transfer of personal data outside the EEA and information should not be transferred outside of the UK unless it meets the requirements of the data protection legislation. Any such transfers require the completion of a DPIA and approval at the board level.

Partners and any third parties working with or for the organisation, and who have or may have access to personal data, will be expected to comply with the principles of this Policy. No third party may access personal data held by the organisation without having first entered into an Information Sharing Agreement (ISA) which imposes on the third-party obligations no less onerous than those to which the organisation is committed, and which gives the organisation the right to audit compliance with the agreement.

An Information Sharing Agreement Addendum to this policy is available if needed on One Drive. This agreement (or a comparable agreement, with all relevant sections) must be completed prior to information sharing commencement.

All **St Helens Mind** projects funded in partnership with other third-party organisations should include within the contractual agreement a clear statement as to the extent to which **St Helens Mind** and the third-party partner organisation is responsible for compliance with data protection legislation (as data controller and/or data processor) and the respective obligations of **St Helens Mind** and the third party partner organisation with regard to data protection.

## Individual's Rights & Data Subject Access Requests (DSARs)

Individuals have the following rights regarding data processing and the data that is recorded about them:

1. The right to be informed about how we use their personal data.
2. The right to access their personal data.
3. The right to rectify their personal data.
4. The right to have their personal data erased.
5. The right to restrict processing.
6. The right to have a copy of their personal data in a portable form.
7. The right to object to direct marketing and profiling.
8. Rights in relation to automated decision making and profiling.

Individuals can request access to their information in line with the rights above. This is called a Data Subject Access Request (DSAR). If you receive a request, you should forward it on to the Data Protection Officer immediately. It is important that this request is passed on to the DPO quickly because **St Helens Mind usually** must respond to a DSAR within one month.

Individuals can make a DSAR verbally or in writing, including via social media. The individual does not need to use specific words or terms to make a request. A third party can make a DSAR on behalf of another person. In this case, additional care must be taken to ensure the legitimacy of the request

and that the third party is entitled to act on behalf of the individual. A third party can also make a request for data regarding a deceased person. This request falls under Freedom of Information legislation (not UK GDPR). However, special care must be taken when responding to these requests, as the records are likely to can information about other (living) individuals whose information is protected by data protection legislation.

When responding to a DSAR, the response must be in a permanent form unless it is not possible, or the individual agrees otherwise. Any unintelligible terms must be explained. The data must not be changed between receipt of the DSAR and sending the information to the applicant, except for routine amendment of the data which would happen in any case.

There are some legal exemptions to the rights detailed above. All DSARs, including any possible exemptions, are coordinated by the Data Protection Officer in conjunction with the relevant office/department.

## Data Protection Procedures

To enact its data protection policy, **St Helens Mind will** implement the procedures below. These procedures should be read in conjunction with the following relevant policies & procedures:

- Confidentiality Policy
- Consent Policy
- Information Breach Policy
- Privacy Policy (public; for clients)
- Staff Privacy Policy
- Records Management & Retention Policy
- IT Security Policy
- Password Policy
- Bring Your Own Device Policy
- Homeworking Policy

### Data Storage

**St Helens Mind stores** information about staff, trustees, volunteers, service users, and other relevant stakeholders on its computers, in a secure cloud-based storage system Office 365. All computers, cloud accounts, and CRM database accounts are password protected and can only be accessed by username and password.

**St Helens Mind 's** Information Technology service provider is **Microsoft Office**, which ensures access to our computers, emails, and cloud-based services are secure.

Physical copies of files containing personal data must be kept in locked filing cabinets and access is restricted to individuals who require this information to carry out their day-to-day work. Keeping files within a locked office is not sufficient protection for personal data. There should be at least two barriers to access. For example, the two barriers for physical files would be the locked office and a locked filing cabinet.

Any individuals routinely working from home or who need to move personal data between locations as part of their routine work should have an appropriately secure data storage system.

### Data Security

As part of ordinary working, personal data pertaining to service users and other stakeholders must be stored securely within **St Helens Mind 's** service user database. Similarly, personnel data must be

stored security within **St Helens Mind 's** personnel database. Personal data should not be stored on individual computers or in paper format, as this is considered the least secure location for data storage.

All staff are responsible for ensuring that any personal data **St Helens Mind holds** and for which they are responsible, is held securely and is not disclosed to any third party unless that third party has been specifically authorised to receive that information.

You must not remove personal data from **St Helens Mind 's** premises either in electronic or paper form unless it is necessary. If data mobility is part of routine working, this must be documented in the Data Map and appropriate security measures must be established.

In instances where data is transported or accessed electronically out of **St Helens Mind 's** premises, the data must be fully encrypted, and password protected. Accessing **St Helens Mind 's** database should be done on a secure internet network (e.g., a password protected network; not a 'public' network).

In some instances, it may be necessary to share personal data with other entitled individuals. When doing this, staff and volunteers should pseudonymise the data as much as possible. Pseudonymisation is a technique that replaces or removes identifying information about an individual. For example, it may involve replacing names or other details that might identify an individual with a **St Helens Mind client** ID number. Staff and volunteers should endeavour to pseudonymise as much as possible but particularly if the data is in paper format or is being communicated electronically (e.g., via email).

## Data Breaches & Near Misses

According to the ICO, a personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed in connection with the provision of a public electronic communications service."

The following are the three most common types of personal data breaches:

I. An *intentional, malicious breach*: The incident resulted from malicious actions such as a theft, computer virus, or unauthorised access where the intent is to cause harm. This is colloquially referred to as "hacking" and is the least likely personal data breach for **St Helens Mind to** experience.

II. An *intentional, not malicious breach*: The incident resulted from non-malicious actions such as disclosure, unauthorised access, or snooping, where the intent was *not* to use the information to cause harm. This type of breach would occur if an individual at **St Helens Mind shared** or accessed personal information when it was not necessary to do so.

III. An *unintentional or inadvertent breach*: The incident resulted from inadvertent actions such as misdirected or accidental emails, unintentional posting or mailing of service user information, or accidentally losing a memory stick or physical copy of a file containing service user information. This type of breach could also occur if an individual accidentally alters or deletes personal data. This is the most common type of personal data breach.

Any individual who becomes aware of a data breach at **St Helens Mind should** notify their line manager and/or the DPO immediately. This is because early detection can allow **St Helens Mind to** minimise or limit the impact of the breach.

In certain circumstances, **St Helens Mind must** notify the ICO as soon as possible and within 72 hours of **St Helens Mind becoming** aware of the breach. **St Helens Mind has** an obligation to assess the likely risk to individuals resulting from the breach. If the risk is deemed to be high, the individuals who are affected must be informed directly and without undue delay. **St Helens Mind must** report a breach on this scale to National Mind as part of its obligations under the Mind Federation Agreement.

In instances where there is a large-scale breach of data, where the data breached will result in a risk to individuals, and/or where the breach may result in reputational risk, the DPO must notify senior leadership and the board of trustees. **St Helens Mind should** establish an action plan to determine how the organisation will respond to the breach and which external organisations or individuals need to be notified.

Not all data incidents are categorised as 'breaches' and might instead be considered 'near misses.' A near miss is a data incident that did not actually result in a breach, although it had the potential to do so. Near misses should also be reported to line managers and/or the DPO as they are opportunities for **St Helens Mind to** examine and learn from its data risk areas.

**St Helens Mind will** keep a log of all data incidents, including breaches and near misses. It will be stored in OneDrive and managed by the DPO. The log should include:

- its causes;
- what happened;
- the personal data affected;
- the effects of the breach; and
- any remedial action taken and rationale

## Data Quality

All individuals at **St Helens Mind are** responsible for ensuring the quality and accuracy of the data that they record and manage. This applies both to information provided by the individual about themselves (i.e., personnel data) and information recorded by the individual on behalf of service users. Due to the nature of the data processed at **St Helens Mind (**i.e., largely health and social care information), **St Helens Mind recognises** that data quality is an iterative process that requires revising, updating, and monitoring to ensure consistency and quality across time.

Data quality is important for the appropriate provision of services, as well as the safety and security of all individuals who engage with **St Helens Mind.** Data quality also fulfils **St Helens Mind 's** obligations under data protection legislation, where all individuals have a right to data accuracy and rectification.

Data quality guidance and training is mandatory for all staff and volunteers when starting at **St Helens Mind as** part of induction and the training schedule. This training includes, but is not limited to, how to use **St Helens Mind 's** database and guidance on what information is required within our systems. Additional support is provided by line managers, as needed.

Data quality is monitored during monthly and quarterly spot checks in preparation for monitoring and evaluation reports. At this time, staff and volunteers will be notified of any identifiable errors or gaps in data quality that need rectifying. As part of this quality review, **St Helens Mind will** also ensure it is only collecting the data it needs and notify the DPO of any data that is no longer needed for secure deletion.

## Data Retention and Disposal of Data

Please see **St Helens Mind 's** Records Management and Retention Policy for more details about the appropriate storage, retention periods, and secure destruction of data held by **St Helens Mind.**

## Using Data for Monitoring & Reporting Purposes

While delivering its services, **St Helens Mind works** in partnership with funders or service delivery partners to collect and process personal data about its service users. This includes collecting monitoring and evaluation data, which allows **St Helens Mind to** track outcomes for individuals and services, ensure services are safe and effective, and to demonstrate its impact. To aid in demonstrating these outcomes, **St Helens Mind compiles** monitoring reports.

A designated staff member, who has the relevant data protection training and skills, should be responsible for compiling reports (whether for internal use or for delivery partners and funders). This is to ensure that any reports compiled follow **St Helens Mind 's** data protection policy and to minimise the risk of data incidents due to lack of knowledge.

In some instances, **St Helens Mind may** need to collect or retain data beyond its original purposes to monitor or track progress across time. For example, if **St Helens Mind wants** to track progress against EDI goals across many years. In these instances, the personal data no longer needs to be attributable to an individual it should be anonymised at the earliest opportunity.

Anonymization involves removing information that could lead to an individual being identified (for example, names and other details which reveal the identity of the individual). Anonymising personal data significantly reduces the risks to individuals if that information is compromised.

If data is retained beyond its original purposes, the DPO must be notified and a record of its processing must be kept in the Data Map.

# Policy Implementation

It is the responsibility of all individuals at **St Helens Mind to** comply with data protection legislation. To ensure all staff, volunteers, and trustees feel comfortable and competent in their responsibilities, **St Helens Mind will** appropriately train individuals to fulfil their roles.

All staff, volunteers, and trustees must read this Data Protection Policy (and other relevant policies, as detailed in the induction policy) when they join **St Helens Mind.** Staff and volunteers who will be handling data during their role must receive training in the following areas prior to starting:

- Data protection principles and procedures
- IT security and procedures
- Understanding confidentiality and consent
- How to use **St Helens Mind 's** service user database (and/or staff database, where relevant)

Staff and trustees who sit on the Data Protection Team, or who hold specific data protection responsibilities, should receive additional specialist training commensurate with their role. The DPO in particular is legally required by UK GDPR to be "independent, an expert in data protection, adequately resourced, and report to the highest management level" (www.ico.org.uk).

Training for all staff and volunteers must be refreshed annually. All individuals at **St Helens Mind are** encouraged to identify any additional training needs during regular supervisions.
This policy and other relevant documentation are stored in One Drive for ease of access.

## Policies Referenced

Please see the additional Data Protection & Security Policies, listed below, for further details about data protection at **St Helens Mind.**

- Confidentiality Policy
- Consent Policy
- Information Breach Policy
- Privacy Policy (public; for clients)
- Staff Privacy Policy
- Records Management & Retention Policy
- IT Security Policy
- Password Policy
- Bring Your Own Device Policy
- Homeworking Policy
- Information Sharing Agreement Addendum

## Version Control

| Date of last edit: | Last Editor: | Approved by: | What changed? | Date of next review |
|---|---|---|---|---|
| Dec 2023 | Paul O'Brien CEO | | New Document | June 24 |
| June 2026 | Paul O'Brien CEO | | Non | June 28 |

# Appendix A

## Lawful Bases for Processing Data

Personal Data
Under the UK GDPR, there are 6 lawful bases for processing non-sensitive personal data:

- **Consent**: The individual has given clear consent for the data owner to process their personal data for a specific purpose.
- **Contract**: The processing is necessary for a contract the data owner has taken with the individual, or because they have asked the data owner to take specific steps before entering a contract.
- **Legal Obligation**: The processing is necessary for the data owner 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 to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
- **Legitimate interests**: The processing is necessary for the data owner's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Stricter rules apply to sensitive personal data. **St Helens Mind will** only collect this information when needed and under specific circumstances. The legal basis for processing sensitive personal data will also be stored in the Data Map.

Special Category Personal Data
Under the UK GDPR, the lawful bases for processing special category data are:

- Explicit consent
- Employment, social security, and social protection (if authorised by law)
- Vital interests
- Not-for-profit bodies
- Made public by the data subject
- Legal claims or judicial acts
- Reasons of substantial public interest (with a basis in law)
- Health or social care (with a basis in law)
- Public health (with a basis in law)
- Archiving, research, and statistics (with a basis in law)

There are also special conditions for processing criminal offence data (e.g., via DBS checking) and this must also be recorded in the Data Map.

Regardless of the type of personal data, the ICO should be consulted for guidance and resources around the legal basis for processing.