Data Protection Policy

A registered Charity in England and Wales (no. 1123615)
Registered Company (no. 06541083)

Contents

1. Introduction

1.1. Purposes

Cwm Taf Morgannwg Mind (**"CTMM"**) is an independent, user focused charity providing quality services to make a positive difference to the wellbeing and mental health of the people of Merthyr Tydfil, Rhondda Cynon Taf and Bridgend.

During Cwm Taf Morgannwg Mind's daily operations, the organisation receives, processes, and shares data relating to service users, staff, volunteers, trustees, stakeholders, donors and any other third parties. CTMM recognises that data security is a key part of providing effective services as well as maintaining integrity and public confidence. The organisation is committed to protecting the privacy and confidentiality of personal data processed during all its activities.

To ensure legal and regulatory responsibilities are met for the use and storage of this data, Cwm Taf Morgannwg Mind has a clear and relevant Data Protection Policy, complying 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 Policy, in line with the Data Protection Legislation is to:

- ✓ To protect the rights and privacy of living individuals who access Cwm Taf Morgannwg Mind's services, work for, or support Cwm Taf Morgannwg 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.
- ✓ To ensure that everyone managing and handling personal data at Cwm Taf Morgannwg 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 with regards to data protection.
- ✓ To engage in best practice around data protection principles and procedures, so that any staff, volunteers, service users, and trustees working with Cwm Taf Morgannwg Mind can feel confident and trusting in our approach to data protection and that Cwm Taf Morgannwg Mind will always act in their best interests.

1.2. Information Commissioner's Office (ICO)

Cwm Taf Morgannwg Mind is registered with the Information Commissioner's Office (ICO), reference number: **Z8567316.**

Cwm Taf Morgannwg 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.

1.3. 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 Cwm Taf Morgannwg Mind, including staff, volunteers, service users, trustees, vendors and suppliers.

At Cwm Taf Morgannwg Mind, this policy applies to all staff, volunteers, trustees, and third-party contractors working with the Organisation. Any person working in these roles should familiarise themselves with this policy and Cwm Taf Morgannwg Mind's IT Security Policy. All of CTMM's policies terms and guidelines must be complied with when processing personal data.

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.

1.4. Data Protection Principles

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

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 or kept for other reasons than the original purposes the personal data has been processed for. 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 (Cwm Taf Morgannwg Mind) is responsible for and must be able to demonstrate compliance with data protection legislation and these principles.

2. How does Data Protection affect me in my role at Cwm Taf Morgannwg Mind?

Cwm Taf Morgannwg Mind encourages staff to view data protection positively, to feel confident in understanding the principles contained in the Data Protection Policy and to feel supported in their day-to-day work.

CTMM could be fined if staff use or disclose information about other people without their consent (or other lawful grounds). To help keep personal data secure, staff should take particular care when using the internet, e-mail, talking on mobile or landline telephones, Lamplight (Cwm Taf Morgannwg Mind's service user database), or using any other database to store company related data. Staff must also adhere to the guidelines regarding security whilst using systems and devices at work in the IT Security Policy.

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. It is an offense to steal or recklessly misuse personal data.

Any breach of Data Protection Legislation or this policy will be dealt with under Cwm Taf Morgannwg Mind's Disciplinary Policy. An intentional breach may also be a criminal offense; in which case Cwm Taf Morgannwg Mind is obligated to report the matter as soon as possible to the appropriate authorities.

3. Definitions

3.1. 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 <u>not considered personal data</u> 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.

3.2. 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.

3.3. Data Controller

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. CTMM is registered with the ICO as a data controller.

4. Roles and Responsibilities

4.1. The Responsibilities of the Board of Trustees

The Board of Trustees is responsible for:

- Reviewing and approving this policy annually.
- Working with the Chief Executive who is the Senior Information Risk Owner (SIRO) to ensure Cwm Taf Morgannwg Mind properly resourced and sufficient budget to fulfil the obligations of this policy.
- Developing a culture of commitment to transparency that informs all the activities of the charity.
- Ensuring personal understanding of UK data protection legislation.

4.2. The Responsibilities of the Chief Executive & Senior Leadership Team (SLT)

The responsibility for compliance with data protection legislation at Cwm Taf Morgannwg Mind rests with the Chief Executive. The Chief Executive is the **SIRO** who "owns" the data protection risk of Cwm Taf Morgannwg Mind.

The Chief Executive is responsible for:

- Ensuring that the organisation complies with UK GDPR and other data protection laws.
- Monitoring of internal compliance, staff training, audits, and
- Managing the data protection policies and procedures of the organisation, and delegating policy improvements to the appropriate member(s) of staff.

- Delegating Data Subject Access Requests (DSARs) to the Head of Service & Deputy CEO.
- Delegating the organisation's improvements of Data Protection to the Finance Manager.
- Reporting data breaches to the ICO and National Mind if appropriate.
- Being the first point of contact to the ICO
- Reporting any potential and live risks to the Board of Trustees.

The Senior Leadership Team (SLT) consisting of the Head of Service & Deputy CEO and the Finance Manager, are responsible to support the Chief Executive in all aspects of data protection essentials for the Organisation.

4.3. The Responsibilities of Managers & Project Leads

All those in managerial or supervisory roles throughout Cwm Taf Morgannwg Mind are responsible for developing and encouraging good information handling practices within the organisation.

Managers and project leads are responsible to ensure that all staff upon induction understand the Data Protection Policy along with all other relevant policies, such as the IT Security Policy, Confidentiality Policy, Code of Conduct Policy, etc. A positive approach must be taken towards the team's understanding of data protection and ensure that any requests for support and/or training are considered appropriately.

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.

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.

The Governance and Corporate Services Lead is responsible for supporting Chief Executive to ensure the organisation complies with current data protection legislation and that all relevant policies are up to date.

4.4. The Responsibilities of all Staff and Volunteers

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

Staff should also ensure they keep their line managers 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 Data Subject Access Requests ("DSARs") that occur.

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

5. Data Processing

5.1. Data Mapping

To demonstrate commitment to the principles above, Cwm Taf Morgannwg 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'). This is available on SharePoint under the "Resources" folder which is accessible to all staff.

Cwm Taf Morgannwg Mind is a data controller under data protection legislation. In some contracts, Cwm Taf Morgannwg Mind works in partnership with organisations as a joint data controller or processor. Because of this, CTMM must ensure that it has a lawful basis for processing personal data.

The lawful basis for processing personal data can be found in **Appendix A**.

5.2. Data Protection Impact Assessments (DPIAs)

Personal data must be protected. Cwm Taf Morgannwg 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 DPIA must be completed and approved.

The ICO provides a DPIA template that is used at Cwm Taf Morgannwg Mind. A copy of this template is stored in SharePoint under the quick access button "Forms & Templates" > "Data Protection Impact Assessment (DPIA)".

5.3. Consent and 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 CTMM to do so.

Cwm Taf Morgannwg 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.

All Cwm Taf Morgannwg Mind services should display or make available adequate Privacy Notices to clients explaining how Cwm Taf Morgannwg Mind processes their information. CTMM 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.

5.4. Data Sharing with Third Parties & Information Sharing Agreements (ISAs)

Cwm Taf Morgannwg 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 Chief Executive.

There are restrictions on the transfer of personal data outside the European Economic Area (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 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 is available in SharePoint under the quick access link "Forms & Templates". Information Sharing Agreement Addendum (template).docx (sharepoint.com) This agreement must be completed prior to information sharing commencement.

All Cwm Taf Morgannwg 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 Cwm Taf Morgannwg Mind and the third-party partner organisation is responsible for compliance with data protection legislation and the respective obligations of Cwm Taf Morgannwg Mind and the third-party partner organisation with regard to data protection.

5.5. 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 (DSAR). Individuals can make a DSAR verbally, via email or in writing, including via social media. All requests must be forwarded on to the Head of Service & Deputy CEO immediately.

Service users must formally fill out an "Authorisation to Release Form". A template of the form is located on SharePoint under the quick access button "Forms & Templates": Authorisation to Release Form.docx. Once this form is complete, the details must be rigorously checked for accuracy on CTMM's databases and authorisation to release must be granted from the Head of Service & Deputy CEO.

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 Head of Service & Deputy CEO in conjunction with the relevant office/department.

Staff must forward all requests in any circumstance to the Head of Service & Deputy CEO or if absent, the Chief Executive.

Cwm Taf Morgannwg Mind must respond to a DSAR's within one month.

6. Data Protection Procedures and Guidelines

6.1. Data Storage

Cwm Taf Morgannwg Mind stores information about staff, trustees, volunteers, service users, and other relevant stakeholders on its computers, in a secure cloud-based storage system **SharePoint** and in a customer relationship management (CRM) system (i.e., **Lamplight** for client data; **Bright HR** for staff data). All computers, cloud accounts, and CRM database accounts are password protected and can only be accessed by username and password. Multi-factor authentication process must be enabled on all databases and sites.

CTMM's Information Technology service provider is **SA1 Solutions** which ensures access to our computers, emails, and cloud-based services are secure. Further specifications, guidelines, appropriate usage and details regarding IT Security can be found in CTMM's IT Security Policy.

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, files being inside a locked office inside a locked filing cabinet. Staff must ensure that physical copies of files have two barriers of protection whether working in head office, remotely or using external storage.

6.2. Data Quality

All individuals at Cwm Taf Morgannwg 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 Cwm Taf Morgannwg Mind (i.e., largely health and social care information), Cwm Taf Morgannwg 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 Cwm Taf Morgannwg Mind. Data quality also fulfils CTMM'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 Cwm Taf Morgannwg Mind as part of induction and the mandatory training schedule. This training includes, but is not limited to, how to use Cwm Taf Morgannwg Mind's database(s) and guidance on what information is required within our systems. Additional support is provided by line managers, as needed. Periodic refresher awareness training is provided by CTMM and staff should request approval for any further appropriate training from their line manager.

Data quality is monitored during 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, CTMM will also ensure it is only collecting the data it needs and ensure that any data that is no longer needed is securely deleted.

6.3. Data Security

As part of ordinary working, personal data pertaining to service users and other stakeholders must be stored securely within Cwm Taf Morgannwg Mind's service user database, Lamplight. Similarly, personnel data must be stored securely within Cwm Taf Morgannwg Mind's personnel databases, Bright HR and SharePoint. Suppliers, vendors and funders details are stored in Sage and Xero Account software. 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 Cwm Taf Morgannwg 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.

Staff must not remove personal data from Cwm Taf Morgannwg 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, and appropriate security measures must be established.

In instances where data is transported or accessed electronically out of Cwm Taf Morgannwg Mind's premises, the data must be fully encrypted, and password protected. Staff can access a tutorial on password protecting documents in SharePoint under "Resources": How to Password Protect a Word Document.mp4 (sharepoint.com)

Accessing Cwm Taf Morgannwg Mind's database should be done on a secure internet network (e.g., a password protected network; not a 'public' network) as outlined in Cwm Taf Morgannwg Mind's IT Security Policy.

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 Cwm Taf Morgannwg 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.

7. 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:

A) 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 Cwm Taf Morgannwg Mind to experience.

B) 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 Cwm Taf Morgannwg Mind shared or accessed personal information when it was not necessary to do so.

C) 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.

7.1. Reporting a Data Breach & Near Miss

Cwm Taf Morgannwg Mind aims to ensure reporting a data breach or a near miss is a simple and straight forward process.

A **data breach** is a security incident that results in the **unauthorised exposure, disclosure, or loss of personal or confidential information.** Not all data incidents are categorised as 'breaches' and might instead be considered 'near misses' (collectively referred to as "incident[s]"). 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 are opportunities for Cwm Taf Morgannwg Mind to examine and learn from its data risk areas.

The data incident procedure for staff when using CTMM's devices and systems as explained in the IT Security Policy is as follows:

1. Firstly, staff must notify SA1 Solutions and their line manager immediately.
When reporting an incident to SA1, this must be reported via the BMS ticketing system which operates 24/7 (newticket@sa1solutions.com) or by contacting the designated security hotline on 01792 464242.

The designated hotline operates from Monday to Friday 8am to 5.30pm and 9am to 12pm on Saturday. This line will not be open on Sunday's or on bank holidays. If the hotline is required outside of its operating hours, incidents can be logged through the BMS ticketing system, which will prioritise the issue for the next operational period.

When reporting a security incident to SA1 Solutions, please provide:

- Your name and contact details for follow up.
- Date and time of detection for the incident.
- A clear description of the issue.
- Actions already taken, such as disconnecting affected devices or locking accounts.
- Details of affected system, users or applications.

2. **Secondly**, the line manager must ensure the staff member completes a "Data Breach and Near Miss Form" and inform the Chief Executive.

All incidents should be reported on an "Data Breach Incident and Near Miss Form" (see **Appendix B**) located on SharePoint under the quick access button "Report an Accident or Incident". Report a Data Breach - Incident and Near Miss Form.docx (sharepoint.com)

The completed form must be shared with the staff member's line manager and the Chief Executive, who will then store completed forms must be stored under the SharePoint folder "SLT" > "Data Breach Incidents and Near Misses".

Cwm Taf Morgannwg Mind will keep a log of all data incidents, including breaches and near misses. It will be stored in SharePoint under "Data Breach Incidents and Near Misses". The log should include:

- Its causes.
- What happened.
- The personal data affected.
- The effects of the breach; and
- Any remedial action taken and rationale.

The Chief Executive will decide if the data incident is appropriate to report to the ICO and/or National Mind (guidance in 6.6 and 6.7).

SA1 Solutions will take *immediate* action to mitigate any damage as a result of a data incident. An investigation will be conducted to inspect the causes and the impact of the incident. Once this has been completed, a response will be provided to CTMM. Staff must ensure that their line manager and the Chief Executive are included in all steps of the incident reporting, investigation and response.

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 Chief Executive must notify the board of trustees. Cwm Taf Morgannwg 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.

If staff are reporting a data breach or near miss that has not happened within CTMM's IT devices and databases that SA1 Solutions provide support with, this should be reported to their line manager immediately. The line manager will ensure that the Chief Executive is informed, and that a "Data Breach and Near Miss Incident Form" is completed.
An investigation will be conducted to determine the causes and the effects of the incident.

The Chief Executive will then decide if it is necessary to report the breach to the ICO and/or National Mind.

7.2. Reporting a data breach to National Mind

Cwm Taf Morgannwg 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. The Chief Executive of Cwm Taf Morgannwg Mind must report a breach on this scale to National Mind via contact with Mind's Network Relations Lead as part of its obligations under the Mind Federation Agreement.

7.3. Reporting a personal data breach to the ICO

If a breach is likely to result in a risk to the rights and freedoms of individuals, The Chief Executive has a duty to report the personal data breach to the Information Commissioner (ICO) within 72 hours of becoming aware of the breach. If left unaddressed, such a breach is likely to have significant detrimental effect on individuals such as:

- Result in discrimination,
- Damage to reputation,
- Financial loss, or
- Loss in confidentiality or any other significant economic or social disadvantage.

Guidance on reporting to the ICO:
If unsure whether or not an incident requires a report to the ICO, the Chief Executive can find guidance on the ICO's website. The ICO have selected examples online taken from various breaches reported to the ICO. These include helpful advice about next steps to take or things to link about: Personal data breach examples | ICO

A live chat with an ICO representative can also be accessed to answer any queries, Monday to Friday, 9am to 5pm (excluding bank holidays): Get help and support from the ICO | ICO.

To report a breach to the ICO:
Before reporting to the ICO, the following information must be readily available:

- **Details of the breach** – a general overview, the date and time it happened and when it was alerted to the Chief Executive.
- **Details of staff member(s) involved** – if a specific member of staff was involved and/or what data protection training they have had.
- **Details of the data and people affected** – how much data and how many people have been affected and the possible risk to individuals as a result of the breach.

- **Your efforts to contain the breach** – what preventative measures were in place beforehand, what actions you've taken to stop it happening again and what other organisations you have told or need to tell about the breach.

Once all information has been collated, an online form must then be filled out on the ICO's website and is available at any time 24/7 (Report a data breach online form | ICO).

Alternatively, a copy of the form can be downloaded via the quick access link "Report an Accident or Incident" > "Report a Data Breach to ICO form - email to icocasework@ico.org.uk.doc (sharepoint.com)" and sent via email to icocasework@ico.org.uk with 'Personal Data Breach Notification' in the subject field.

8. Record Management, Data Retention and Disposal of Data

Cwm Taf Morgannwg Mind has a responsibility to maintain its records ("data") and record keeping system in accordance with the regulatory environment with no ambiguity regarding responsibility for the maintenance and disposal of records.

Cwm Taf Morgannwg Mind stores data in the following databases (online CRM systems):

- Lamplight for client data.
- SharePoint for Organisational data.
- Bright HR for staff data.

8.1. Management of Records

The SLT have overall responsibility for the management of records generated and held within their area, ensuring all records have an identified owner responsible for their management whilst in regular use, and for appropriate retention and disposal.

All members of staff are responsible for ensuring their work is documented appropriately, that the records which they create or receive are accurate and managed correctly and are maintained and disposed of in accordance with Cwm Taf Morgannwg Mind's guidelines and any legislative, statutory and contractual requirements. Line managers should ensure that when a staff member leaves, responsibility for their records is transferred to another person; if any of the information is redundant, it should be deleted by either the departing member of staff or their line manager.

In the management of records:

- Records must be accurate and complete, so that it maintains integrity and so it is possible to establish what has been done and why.
- The quality of records must be sufficient to allow staff to carry out their work efficiently, demonstrate compliance with statutory and regulatory requirements and ensure accountability and transparency expectations are met.
- Staff must ensure records are not duplicated as this presents enhanced risks regarding their management, use and alteration.
- Records must be organised in a uniform, logical manner that facilitates fast, accurate and comprehensive retrieval.
- Where the records are stored, appropriate levels of security and access must be in place to prevent the unauthorised or unlawful use and disclosure of information. All records in any format must be held in accordance with Cwm Taf

Morgannwg Mind's IT Security Policy. Multi Factor or Two factor authentication must be activated. For further guidance, advice must be sought from staff's line manager and/or via SharePoint's quick access link "Cyber Security & 2FA": Cwm Taf Morgannwg Mind - Cyber Security - All Documents (sharepoint.com)

8.2. Data Retention

The Freedom of Information Act Section 46 Code of Practice on the Management of Records states:

"As a general principle, records should be kept for as long as they are needed by the authority: for reference or accountability purposes, to comply with regulatory requirements or to protect legal and other rights and interests. Destruction at the end of this period ensures that office and server space are not used, and costs are not incurred in maintaining records that are no longer required".

Records must only be kept for as long as is required to meet operational, business and legal needs. It is a legal requirement established by the Data Protection Act to only retain records containing personal data for as long as is strictly necessary, and Cwm Taf Morgannwg Mind can be subject to enforcement action for failing to comply.

8.3. Disposal of Data

Line Managers are responsible for ensuring that when the appropriate data reaches the end of its retention period, a decision must be taken on its disposal. The SLT must approve its destruction. All copies, including security copies, preservation copies and backup copies held in any format must be destroyed at the same time.

If confidential data in paper form is to be destroyed, this must be disposed of by shredding and then emptied into the white sacks available in Cwm Taf Morgannwg Mind's head office.

Records and any data held on Lamplight can be deleted by users with "Project Administrator", "System Administrator" or "Manager" access rights. Guidance when using Lamplight can be found under SharePoint's quick access link "Lamplight Guidance" > "Lamplight Help Manual": Lamplight Help Manual.docx (sharepoint.com).

Staff with access to digital records that are being deleted should ensure that any copies held anywhere in their email folders, files stores and recycle bin are also deleted to ensure completion.

Exception: Data must not be destroyed if any litigation, claim, negotiation, audit, Freedom of Information or Data Protection request, administrative review, or other action involving the relevant information is initiated before the expiration of the retention period. They must be retained until the completion of the action and the resolution of all issues that arise from it, or until the expiration of the retention period, whichever is later.

9. Using Data for Monitoring & Reporting Purposes

While delivering its services, Cwm Taf Morgannwg 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 Cwm Taf Morgannwg 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, Cwm Taf Morgannwg 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 Cwm Taf Morgannwg Mind's Data Protection Policy and to minimise the risk of data incidents due to lack of knowledge.

In some instances, Cwm Taf Morgannwg Mind may need to collect or retain data beyond its original purposes to monitor or track progress across time. For example, if Cwm Taf Morgannwg Mind wants to track progress against Equality, Diversity and Inclusion (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.

Anonymisation 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 senior leadership team must be notified.

10. Policy Implementation

It is the responsibility of all individuals at CTMM to comply with the Data Protection Policy and all relevant data protection legislation. This policy will be reviewed annually by the Board of Trustees.

All staff, volunteers, and trustees must read this Data Protection Policy (and other relevant policies) when they join Cwm Taf Morgannwg 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 Cwm Taf Morgannwg Mind's service user database (and/or staff database[s], where relevant).

This policy will be available to view at any time on CTMM's SharePoint site under the quick access button "Policies & Procedures".

To ensure all staff, volunteers, and trustees feel comfortable and competent in their responsibilities, Cwm Taf Morgannwg Mind will appropriately train individuals to fulfil their roles. Training for all staff and volunteers must be refreshed annually. Staff, volunteers and trustees are responsible for completing all mandatory training assigned in the specified completion time frame. All individuals of Cwm Taf Morgannwg Mind are encouraged to identify any additional training needs during regular supervisions.

11. Version Control

Change Control	
Version:	V1.0
New / Replacement or Updated:	New
Approved by:	Board of Trustees
Date Approved:	28th November 2024
Author:	Governance and Corporate Services Lead
Date Issued:	28th November 2024
Review Date:	November 2025
Reviewed by:	Board of Trustees

Revision History			
Version	**Type**	**Date**	**History**
V1.0	New	22.10.24	

There may be occasions where it has not possible to review this policy within the timescale indicated above, such as where there are imminent legislative changes, and in these cases the existing policy will remain valid until renewal.

12. Acknowledgment of Data Protection Policy

I acknowledge that I have read and understand my responsibilities laid out in the Cwm Taf Morgannwg Mind Data Protection Policy.

Signed	
Name	
Date	

In the event a wet signature cannot be obtained, a signature can be given virtually via a "read receipt" or written confirmation of acceptance via email. All signed forms will be stored on staff's Bright HR accounts under "Documents" and for the Board of Trustees in SharePoint by the Governance and Corporate Services Lead.

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. **Cwm Taf Morgannwg Mind** will only collect this information when needed and under specific circumstances.

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.

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

Appendix B

mind Cwm Taf Morgannwg

Data Breach Incident and Near Miss Form

Incident Date		**Incident Time**	
Location		**Date/Time Reported**	
Staff Member Involved			
Incident that affected: (delete as appropriate)	Staff / Service User / Volunteer		
Incident Reference Number (DD/MM/YY+initials of staff member involved)			

Details of Incident/Near Miss

The Personal Data affected

The effects of the breach/near miss

Remedial Action Taken and Rationale (to be completed by line manager)

Report Completed by		**Date**	
Line Manager		**Date**	
Signature			

Once complete, line managers must store this report in SharePoint: SLT > Data Breach Incidents & Near Misses.

Once stored, line Managers must fill in the "Data Breach Incidents & Near Misses Log" with all information gathered.