DATA PROTECTION & CONFIDENTIALITY POLICY

THE ARTHUR ELLIS MENTAL HEALTH FOUNDATION

Purpose

The nature of the work undertaken by AEMHF requires us to gather information about clients and to keep clinical notes on sessions. These notes will be updated following every session, to ensure a record of any support given and any concerns raised are recorded.
In addition, any safeguarding concerns and behaviour issues are also recorded, to aid in the assessment of risk to both client and staff.
There are occasions where AEMHF will be required to share this information with relevant agencies, in order to keep clients safe.

Scope

This policy relates to the protection of Personally Identifiable Data (herein referred to as personal data), that is any piece of data that could identify an individual such as their name, address, date of birth, telephone number, parent's/carer's names, email address.
This personal data must be handled in an appropriate manner, whether in paper form or online, to protect the privacy for those which it concerns.

AEMHF regards the lawful and correct treatment of personal data of paramount importance. All individuals associated with our service, children, carers, staff, students and volunteers, have a right to expect that their personal data is treated lawfully and respectfully. To ensure this we adhere to the principles of the General Data Protection Regulations (GDPR) 2024 and subsequent UK guidelines for the collection and processing of personal data.

The GDPR principles (Article 5) requires that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Collected for specified explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

REVIEW

Written: January 2025
Adapted: September 2026
For review: September 2027
Updated on Website: September 2026

Scope Cont.

5.Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
6.Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In addition, Article 5 (2) requires that:

- The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

(Source: The Information Commissioner's Office)

Procedure

We are registered with the Information Commissioner's Office (ICO) – registration number C1469107. We have appointed Jon Manning as the Data Protection Officer for our AEMHF. The responsibilities include the provision of privacy statements, updating this (and related) policies on an annual basis, undertaking regular audit of our data protection systems and processes, monitoring staff with regards to appropriate handling of data and ensuring systems are in place to maintain the accuracy of the data we hold.

REVIEW

Written: January 2025
Adapted: September 2026
For review: September 2027
Updated on Website: September 2026

Procedure Cont.

- We ensure that we share information with those who receive support from AEMHF, parents/carers and other agencies who come into contact with us, this includes details of how we:
- Meet the GDPR regarding the collection of their personal data.
- Fulfil our obligations to specify our lawful basis for processing their data and the purposes for which it will be used.
- Collect and process only appropriate data that is required to fulfil the operational needs of the business and to comply with legislation.
- Ensure the quality of the data used and that it is timely, accurate and kept up to date.
- Ensure those associated with our service are fully communicated to regarding their right to be informed that data collection and processing is undertaken, to their right of access to their personal information, their right to withdraw consent (where given) and their right to be forgotten and to correct, rectify, block or erase inaccurate data.
- Set out transparent procedures for responding to requests for information.
- Share information appropriately, detailing whom we may share with and the circumstances for doing so.
- Store both current and historical data.
- Ensure staff receive training and guidance in our processes for handling personal data.
- Staff are appropriately supervised when handling personal data.
- Breaches of data protection by staff may lead to disciplinary action being taken by our service.
- A data audit is carried out annually by the Data Protection Officer with the purpose of identifying the data held, our lawful basis for processing, the systems and processes in place to ensure the accuracy of the data and the identified retention periods of historical data.
- Where information is held on an external system, such as the cloud, we ensure those organisations have a Data Sharing Policy detailing how they protect the data provided. This is made available to clients, parents/carers, staff, volunteers and organisations we work with upon request.
- Our email systems are encrypted to prevent unauthorised access to any data shared by this means (see our Acceptable Internet Use Policy).
- Our secure recording systems and electronic devices are password protected to prevent unauthorised contact.

REVIEW

Written: January 2025
Adapted: September 2026
For review: September 2027
Updated on Website: September 2026

Procedure Cont.

- Clients, parents/carers, staff and volunteers within our service have a right to know that the data shared with us will be regarded as confidential, as well as to be informed of the circumstances when, and the reasons why, we may be obliged to share information either with or without consent.
- We are obliged to share information without authorisation from the person who provided it, or to whom it relates, when:
- There is evidence that a child is suffering, or is at risk or suffering, significant harm.
- There is reasonable cause to suspect that a child may be suffering, or is at risk of suffering, significant harm.
- It is to prevent a crime from being committed or to intervene where one may have been.
- Not sharing the information could be worse than the outcome of having shared it.
- A vulnerable adult is unable to protect themselves and is at risk of harm.
- A vulnerable adult has a mental health capacity assessment which indicates that they are unable to understand the risks and protect themselves.

Information Storage

AEMHF will only store information that is relevant to undertake its core work. This will include personal information about the client, their circumstances, any vulnerabilities and the reason for the referral. It will also include details and contact details for other agencies such as school/colleges and GP services.
All information is kept on a secure system on the cloud, information and client notes can be added by any member of staff, they cannot see any safeguarding concerns that have been raised previously. Staff can only have access to personal data of clients that they are directly working with.
The DSL team can see all information and may choose to share it with staff on a case by case basis, depending on the need to know.
In the event of a referral due to safeguarding issues, they will share information with the MASH team and the school/college they are attending (if relevant). On most occasions, this will be shared with client and parent/carer before it happens, providing it is safe to do so.
If it is not safe to share this information and puts the child at risk or creates a flight risk, then it will clearly be recorded on file, why this information must not be shared with the parent/carer.
In the event of it being unclear, then independent legal advice must be sought and recorded on file.

REVIEW

Written: January 2025
Adapted: September 2026
For review: September 2027
Updated on Website: September 2026

Requests for Information

Clients, carers, staff and volunteers have a right to access their personal data and request that any inaccurate data is rectified and/or deleted. All such requests to access the information held on an individual should be made, in writing, to the Data Protection Officer.

Stage One
If there are concerns relating to the way your personal data is handled this should be raised in the first instance with the Data Protection Officer for AEMHF. A verbal request must be followed up by a formal request for access to information held on an individual (yourself or your child) which should be made to the Data Protection Officer.
The Data Protection officer will respond, in writing to acknowledge the request within 10 working days.(Email or letter)
The acknowledgment should include:

- Who the information is about.
- What has been requested.
- Confirmation if information is held or not.
- Confirmation that a response will be made within one month of the request.
- Confirmation that the request meets legal requirements. i.e. is the requester entitled to this information.

Stage Two
The Data Protection officer should check the records requested; all records must be scrutinised taking the following elements into account:

- Information that puts the child at risk must not be shared.
- Information naming other children or staff must be redacted.
- Information directly relating to another child or adult cannot be shared.

The information must be prepared ready to share with the requestor.
A decision will need to be made about how this information will be shared either

- A meeting, where information can be shared face to face.

or

- Copies of information sent to requestor.

REVIEW

Written: January 2025
Adapted: September 2026
For review: September 2027
Updated on Website: September 2026

Requests for Information Cont.

Stage Three
If you are still dissatisfied after receiving the information, you can initially come back to the Data Protection Officer for further clarification.
If you feel that the information is not accurate, then you can request a formal amendment of the data or for an entry to be made detailing what information is in dispute. This must be included on the file and shared when any investigation or formal request for information is requested.
Amendments can only be made to factual information, which is inaccurate, prejudiced or untrue.

Stage Four
If you are still dissatisfied then you can make a complaint to the Information Commissioner's Office (ICO) by writing to Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or via their website ico.org.uk.
This only applies to lack of information being shared by AEMHF with the requestor.

Data Retention

AEMHF do not want to keep any information that is not necessary. However, it is often, only with hindsight that this becomes obvious. We legally should keep child protection records from DOB to when the child turns 25 years.
However, the nature of the files kept online by AEMHF, means they are also the client file showing records of support provided.
This means that currently there is no time limit on keeping these files. AEMHF will not currently hold files that are 25 years old. In future, these files will need to be archived once the child is no longer a client and destroyed when the child turns 25 years.
The DSL is responsible for ensuring that files are securely destroyed, when the child turns 25 years.

REVIEW

Written: January 2025
Adapted: September 2026
For review: September 2027
Updated on Website: September 2026

Devices Used by Staff

AEMHF reserves the right to access and monitor the use of all its owned digital devices, including monitoring internet, telephone, and email use. We also monitor access to our networks via private devices.

Staff must not use the AEMHF internet connections or devices to access content that is illegal, pornographic, or supports hate and/or discrimination. All those representing AEMHF must take the appropriate steps to guard against unauthorised access to, alteration, accidental loss, disclosure, or destruction of data.
Sensitive information pertaining to AEMHF and/or its clients must not be stored on any personal devices.

Storage of information is all on the secure system storage should be kept to a minimum and must not impact on the performance of the network or device.

Any hardware and software provided by AEMHF is only to be used by authorised AEMHF staff and can only to be used in relations to their roles within the organisation. Therefore, to prevent unauthorised access of any system or personal data, you must never leave any information system unattended without logging out or locking the login. To do so would be considered negligent and may lead to disciplinary action being taken. You are not allowed to take your work IT equipment and/or work phone on annual leave with you. This will be considered a breach to data protection.

If using AEMHF property, you must not install or download any software, including browser toolbars or hardware without permission.

AEMHF staff take all possible measures necessary to protect data and information systems from infection, unauthorised access, damage, loss, abuse, and theft.

AEMHF may monitor and record your use of information systems, internet, and email to ensure policy compliance. You must use any equipment professionally, lawfully and in an ethical manner,

REVIEW

Written: January 2025
Adapted: September 2026
For review: September 2027
Updated on Website: September 2026

Devices Used by Staff Cont.

Under the Computer Misuse Act 1990 it is unlawful to gain access to unauthorised computer material, and the intent to commit or facilitate the commission of further offences or modify computer or delete material without authorisation. This also included the bypassing of any filtering and/or security system that are in place.

All client information must be held in accordance with AEMHF policies and procedures, Data Protection Act 2024 and GDPR 2018. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purpose, held no longer than necessary, and will be kept private and secured with appropriate security measures in places; whether it is used in the workplace, hosted online, or accessed remotely,

No personal information like personal photos, files, or financial information should be stored on devices belonging to AEMHF. Only documents related to your role, should be stored on AEMHF devices and systems.

You will respect copyright and intellectual property of AEMHF.

Staff must not create, transmit, display, publish or forward any material that is likely to cause offence, harass, inconvenience, impact on another's mental health and/or bring AEMHF into disrepute.

Volunteers who have access to the AEMHF network and personal data are required to confirm they have reviewed and understand the Privacy Policy.

Employees are responsible for taking care of any equipment they are loaned, any damage to Company property through misuse, recklessness or carelessness may lead to staff being required to repay to the Company the cost of repair or replacement.

The Company reserves the right to recover this cost by way of a deduction from your next salary payment.

If employee's employment is terminated, employees should return all Company property, including IT equipment, stationery, Company mobile phone or tablet, and any other items belonging to the company.

AEMHF are not responsible for the loss, theft or damage to any personal property brought by employees on to Company premises. Employees are responsible for the security and safety of their personal possessions at all times.

REVIEW

Written: January 2025
Adapted: September 2026
For review: September 2027
Updated on Website: September 2026

Devices Used by Staff Cont.

Email & Internet Usage

Staff will be allocated an email address for AEMHF. This is the only email that should be used to communicate with clients. Staff must check their email on a regular basis.

·Staff will be create supplied with a strong password to use with the secure system, they should not change, divulge or share their password with anyone else.

- Staff are responsible for any activity which occurs within their accounts.
- AEMHF retain the right to check any emails used for AEMHF work purposes.
- Email facilities are provided for the purposes of our business, we understand that you may occasionally receive personal emails on the system. As much as possible staff should keep personal and business life separate.
- Employees are not permitted to send personal emails during work time unless in the case of an urgent matter when you should seek the approval of your line manager before sending the email.
- Employees are not permitted to use the internet during work time unless in the case of an urgent matter when you should seek the approval of your line manager before use.
- Employees may use the internet during break times. This is permitted on condition that all the procedures and rules set out in the Company's Code of Conduct are complied with.

The Company will not tolerate use of email and internet unofficial or inappropriate purposes, including:

- Any messages that could constitute bullying, harassment or other detriment.
- Accessing social networking sites such as Facebook using Company equipment or during work time.
- On-line gambling.
- Accessing or transmitting pornography.
- Accessing other offensive, obscene, or otherwise unacceptable material.
- Transmitting copyright information and/or any software available to the user.
- Posting confidential information about other employees, AEMHF or its clients.

REVIEW

Written: January 2025
Adapted: September 2026
For review: September 2027
Updated on Website: September 2026

Social Networking

Social Networking has become common practice. This means that staff, clients and their families are likely to have social media accounts.
AEMHF uses social media to promote its services and support that is available. Staff may also engage in professional forums where they have opportunities to share ideas and engage in discussions on these social networks.
The WhatsApp group also enables discussion, collaboration and debate across the organisation. Names of clients should not be mentioned within these discussions and information must be kept confidential within the group. If other staff do identify an individual, this must not be shared outside of the group.
It is forbidden to connect with clients on social media. Posting or making any comment or engaging in discussions which would adversely affect AEMHF or its reputation, or that of our beneficiaries and suppliers is not permissible.

Staff must not breach discrimination legislation, or harass or bully an employee, volunteer, trustee, ambassador, or damage working relationships between fellow employees, volunteers, trustees, or ambassadors.

When acting on AEMHF business or representing AEMHF we ask that staff and volunteers always consider if communication and response to personal messages is appropriate. If uncertain of how to reply, always refer them onto your Line Manager, Director or a Trustee.

All complaints must either be referred to the Director, who will send details about the complaints procedure or directed to the complaints policy on the website.

Staff are personally responsible for all content posted on their personal accounts and are reminded that regardless of the social network used, or level of privacy settings activated, everything posted onto the internet has the potential to become public and widespread.

Should we have any concern regarding social media connected to an employees' account or in reference to AEMHF, we will discuss this with them in the first instance. Repeated and serious offences could lead to disciplinary action being taken.

REVIEW

Written: January 2025
Adapted: September 2026
For review: September 2027
Updated on Website: September 2026

Social Media

All Social media use for work purposes is overseen and managed by the CEO, Jon Manning. Social media is used to promote AEMHF and to suggest good practice and support available. All posts from employees must be approved to ensure it meets the expectations in terms of focus, language and content. Staff must not engage in inappropriate use of social media networking sites which may bring yourself or AEMHF into disrepute.

Staff should be aware that they leave themselves open to charge of professional misconduct if they publish compromising images and/or demeaning statements of AEMHF staff or clients.

Staff must not share any confidential or sensitive information relating to AEMHF on social media.

Posts on social media, business or personal accounts, must not:

- Compromise the Company, disclose confidential data or disclose sensitive data damaging the Company's reputation or brand.
- Breach laws on copyright or data protection.
- Contain content that is of a libellous or defamatory nature.
- Engage in bullying or harassment.
- Be of illegal, inappropriate or offensive content.
- Interfere with your work commitments.
- Use the Company's name or reputation to promote any other product or any political opinions.
- Employees should ensure they consider the Company's other policies on marketing, promotion, sales, and branding.

REVIEW

Written: January 2025
Adapted: September 2026
For review: September 2027
Updated on Website: September 2026

Data Breaches

There may be occasions where information is shared inappropriately or with a person who is not authorised to receive it.
Any accidental or deliberate breaches of inform must in the first instance be reported to the data protection officer.
The data protection officer is required to report any breaches to the Information Commissioner's Office (ICO) by writing to Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or via their website ico.org.uk
This may lead to further investigation or action being taken by the ICO against AEMHF.

Data Breaches

All information gained during your employment is expected to be considered confidential, during your employment and post-employment. Employees are expected to keep this information confidential, unless required by law not to do so.

All AEMHF staff sign a 'non-disclosure agreement', and all client information is kept in accordance with AEMHF protocols, Data Protection Act 2024 and GDPR 2018.

Staff must not reveal confidential information about AEMHF, its staff, and clients except to those colleagues who have a professional role (and on a need-to-know basis). This includes intellectual property.

Client information must not be discussed outside AEMHF nor used to advance any other practice or service.

Session content must not be discussed with anyone except the DSL and/or during professional supervision and only if appropriate. Occasionally you may be asked to anonymise a case, to allow it to be used as a case study or theoretically.

All staff must be familiar with the Caldicott Principles (see appendix 1) and understand that safeguarding concerns may mean it is appropriate or essential to breech confidentiality. Clients are made aware of this at the commencement of the support.

REVIEW

Written: January 2025
Adapted: September 2026
For review: September 2027
Updated on Website: September 2026

Appendix 1

Principle	Descriptor
Principle 1: Justify the purpose(s) for using confidential information	Every proposed use or transfer of confidential information should be clearly defined, scrutinised, and documented, with continuing uses regularly reviewed by an appropriate guardian.
Principle 2: Use confidential information only when it is necessary	Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.
Principle 3: Use the minimum necessary confidential information	Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.
Principle 4: Access to confidential information should be on a strict need-to-know basis	Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.
Principle 5: Everyone with access to confidential information should be aware of their responsibilities	Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.
Principle 6: Comply with the law	Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.
Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality	Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators, and professional bodies.
Principle 8: Inform patients and service users about how their confidential information is used	A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant, and appropriate information – in some cases, greater engagement will be required.

REVIEW

Written: January 2025
Adapted: September 2026
For review: September 2027
Updated on Website: September 2026

ARTHUR ELLIS
CHARITY NUMBER 1207350

