Address: Linden Heights,
58 Cronks Hill Road,
Redhill
Co. Surrey,
RH1 6LZ.

E: admin@amfmep.co.uk
T: +44 (0)1737 420289

AMF MECH LTD
DATA PROTECTION POLICY:

1. Introduction

This Data Protection Policy is the overarching policy for data security and protection for AMF Mech Ltd (hereafter referred to as "us", "we", or "our").

2. Purpose of the policy

The purpose of the Data Protection Policy is to support the 10 Data Security Standards, the General Data Protection Regulation (2016), the Data Protection Act (2018), the common law duty of confidentiality, and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

This policy covers.
Our data protection principles and commitment to common law and legislative compliance.
procedures for data protection by design and by default.

3. Scope

This policy includes in its scope all data that we process either in hardcopy or digital copy, this includes special categories of data.
This policy applies to all staff, including temporary staff and contractors.

4. Policy Principles

4.1 We will be open and transparent with service users and those who lawfully act on their behalf in relation to their care and treatment. We will adhere to our duty of candour responsibilities as outlined in the Health and Social Care Act 2012.

4.2 We will establish and maintain policies to ensure compliance with the Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the General Data Protection Regulation, and all other relevant legislation.

4.3 We will establish and maintain policies for the controlled and appropriate sharing of service user and staff information with other agencies, taking account all relevant legislation and citizen consent.

4.4 Where consent is required for the processing of personal data, we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time through processes which have been explained to them and which are outlined in our Record Keeping Policy: Withdrawal of Consent procedures. We ensure that it is as easy to withdraw as to give consent.

4.5 We will undertake / commission delete as appropriate annual audits of our compliance with legal requirements.

4.6 We acknowledge our accountability in ensuring that personal data shall be:

4.6.1 Processed lawfully, fairly and in a transparent manner.

4.6.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

4.6.3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

4.6.4. Accurate and kept up to date.

4.6.5. 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 ('storage limitation').

4.6.6. Processed in a manner that ensures appropriate security of the personal data.

4.7 We uphold the personal data rights outlined in the GDPR.

4.7.1. The right to be informed.

4.7.2. The right of access.

4.7.3. The right to rectification.

4.7.4. The right to erasure.

4.7.5. The right to restrict processing.

4.7.6. The right to data portability.

4.7.7. The right to object.

4.7.8. Rights in relation to automated decision making and profiling.

5. Underpinning policies & procedures

These policies and procedures are aligned with those which are requirements in the Data Security and Protection Toolkit (www.dsptoolkit.nhs.uk). It is up to each organisation to assess whether they are necessary – for example, there is no need to have a Network Security Policy if you do not have a network. If you have policies which contain the same information, but which have different names then that's also fine.

- This policy is underpinned by the following:
- Data Quality Policy – outlines procedures to ensure the accuracy of records and the correction of errors.
- Record Keeping Policy – details transparency procedures, the management of records from creation to disposal (inclusive of retention and disposal procedures), information handling procedures, procedures for subject access requests, right to erasure, right to restrict processing, right to object, and withdrawal of consent to share.
- Data Security Policy – outlines procedures for the ensuring the security of data including the reporting of any data security breach.
- Network Security Policy – outlines procedures for securing our network.
- Business Continuity Plan –outlines the procedures in the event of a security failure or disaster affecting digital systems or mass loss of hardcopy information necessary to the day to day running of our organisation.
- Staff Data Security Code of Conduct - provides staff with clear guidance on the disclosure of personal information.

6. Data protection by design & by default

We recognise that this will be new for much of the sector. There is extensive guidance from the Information Commissioner's Office here – please note that this is not sector specific.

- We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.
- We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.
- It is unlikely that any small organisation will be required to undertake a data protection impact assessment. Though it is considered best practice to do one for your care plans at a minimum. Prior to starting any new data processing, we will assess whether we should complete a Data Protection Impact Assessment (DPIA) using the ICO's screening checklist: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.
- All new systems used for data processing will have data protection built in from the beginning of the system change.

- All existing data processing has been recorded on our Record of Processing Activities. Each process has been risk assessed and is reviewed annually.
- We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.
- In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for, and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.
- Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

7. Responsibilities

You should update the responsibilities below based on what makes sense for your organisation, the following are suggestions. There should be an individual who deals with data security and protection day-to-day as part of their job and someone at senior management/board level who is responsible for data security and protection as well. Please note that a Data Protection Officer has specific legal requirements in the GDPR. Do not call someone a DPO unless you are satisfied that they can fulfil their legal requirements.

- Our designated Data Security and Protection Lead is AMF. The key responsibilities of the lead are:
- To ensure the rights of individuals in terms of their personal Darina ta are upheld in all instances and that data collection, sharing and storage is in line with the Caldicott Principles.
- To define our data protection policy and procedures and all related policies, procedures, and processes and to ensure that sufficient resources are provided to support the policy requirements.
- To complete the Data Security & Protection Toolkit (DSPT) annually and to maintain compliance with the DSPT.
- To monitor information handling to ensure compliance with law, guidance and the organisation's procedures and liaising with senior management and DPO to fulfil this work. Please see the note above regarding DPOs and if they are relevant to your organisation.
- If applicable: Our designated DPO is insert name here, they can be contacted via email: insert here; phone: insert here; or at the following address: insert here.
- The key responsibilities of the DPO are:
- Overseeing changes to systems and processes.
- Monitoring compliance with the GDPR and the Data Protection Act 2018.
- Completing DPIA.
- Reporting on data protection and compliance with legislation to senior management.
- Liaising, if required, with the Information Commissioner's Office (ICO).

8. 8. Approval

8.1. This policy has been approved by the undersigned and will be reviewed annually.

SIGNED BY

Adam Fleming Company Director
for and on behalf of AMF Mech Ltd

.....

Signed Date: .....10/08/2025.....

Expiry Date: .....10/08/2026.....

AMF MEP