Data Privacy and Cyber Protection Policy

1. Introduction

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

2. Purpose

2.1. 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.

2.2. 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

3.1. This policy includes in its scope all data which we process either in hardcopy or digital copy, this includes special categories of data.

3.2. This policy applies to all staff, including temporary staff and contractors.

4. 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 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.

Due to our size, we have determined that we are not required to have a Data Protection Officer (DPO), as we do not process special categories of data on a large scale. Nonetheless, to ensure that individuals' data rights are respected and that there are the highest levels of data security and protection in our organisation, we have appointed a member of staff to be our Data Security and Protection Lead. The Data Security and Protection Lead will report to the highest management level of the organisation. We will support the Data Security and Protection Lead with the necessary resources to carry out their tasks and ensure that they can maintain expertise.

5. Data protection by design & by default

5.1. 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.

5.2. 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.

5.3. 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.

5.4. All new systems used for data processing will have data protection built in from the beginning of the system change.

5.5. All existing data processing has been recorded on our Record of Processing Activities. Each process has been risk assessed and is reviewed annually.

5.6. We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

5.7. 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.

5.8. Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

6. Responsibilities

6.1. Our designated Data Security and Protection Lead is Lara Peat. The key responsibilities of the lead are:

6.1.1. To ensure the rights of individuals in terms of their personal data are upheld in all instances and that data collection, sharing and storage is in line with the Caldicott Principles.

6.1.2. 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.

6.1.3. To complete the Data Security & Protection Toolkit (DSPT) annually and to maintain compliance with the DSPT.

6.1.4. To monitor information handling to ensure compliance with law, guidance and the organisation's procedures and liaising with senior management to fulfil this work.

6.2. Other key responsibilities are:

6.2.1. Overseeing changes to systems and processes.

6.2.2. Monitoring compliance with the GDPR and the Data Protection Act 2018.

6.2.3. Completing DPIA.

6.2.4. Reporting on data protection and compliance with legislation to senior management.

6.2.5. Liaising, if required, with the Information Commissioner's Office (ICO).

7. Administrator Accounts

7.1 Administrator privileges shall only be granted where there is a documented business requirement and approval has been provided by the Managing Director or another authorised senior manager.

7.2 Each individual requiring administrative access shall be assigned a separate administrator account. Administrator accounts must not be shared between users.

7.3 Standard user accounts shall be used for all routine day-to-day activities, including email, web browsing, document creation, and other non-administrative tasks.

7.4 Administrator accounts shall only be used to perform administrative activities, such as installing or removing software, changing system configurations, managing user accounts, or carrying out maintenance tasks.

7.5 Administrator accounts must not be used for routine internet browsing, email, or other activities that could unnecessarily expose administrative privileges to security threats.

7.6. In instances where cloud-based services are utilised, we will ensure that management of such platforms is conducted via dedicated administrative profiles, which must remain entirely separate from regular user credentials.

7.7. We will conduct reviews of administrative permissions at minimum once per year or upon any transition in personnel roles. We will revoke elevated access rights immediately once the business necessity concludes.

7.8. We are committed to the principle of least privilege, ensuring that administrative accounts are only provided with the baseline level of entry required to fulfill sanctioned obligations.

7.9. A current inventory of all accounts with elevated privileges shall be maintained by us. This documentation will include the identity of the user, specific system access, formal business case, management sign-off, and the date of provision. This record will undergo an annual audit to confirm ongoing suitability of access.

8. Multi-Factor Authentication (MFA)

8.1. We shall activate Multi-Factor Authentication across all cloud-hosted solutions and profiles where such security features are technically compatible.

8.2. The use of MFA is a compulsory requirement for every administrative account, whether situated on local hardware or within cloud environments.

9. Passwords and Passkeys

9.1. Robust authentication methods shall protect every user account. We advocate for the adoption of passkeys over traditional passwords where possible to enhance our defenses against credential misappropriation and phishing attempts.

9.2. In circumstances where password-based entry is required, we mandate that these be distinct for every profile and strictly prohibited from being recycled across different platforms.

9.3. We require that all passwords possess a character length sufficient to maintain high-level security standards.

9.4. No password shall be recorded in physical writing or kept in a non-secure format. We support the utilization of sanctioned password management tools for the creation and encrypted storage of unique credentials.

9.5. We will replace any factory-set or vendor-supplied default passwords with secure alternatives prior to the deployment of any device or service into our operational environment.

9.6. Should there be any suspicion of unauthorized exposure or compromise, passwords must be updated without delay. Any such event will be formally documented within the Data Security Incident Register.

10 Software Updates and Supported Software

10.1 Automatic security updates shall be enabled wherever this functionality is available and appropriate.

10.2 Where automatic updates are not available, all security updates and vulnerability fixes for operating systems, applications, routers, firewalls, and other supported software shall be applied within 14 days of release.

10.3 All software and operating systems used by the organisation must be supported by the vendor and continue to receive regular security updates and vulnerability fixes.

10.4 Software that is no longer supported by the vendor, or no longer receives regular security updates or vulnerability fixes, shall be removed from all company devices immediately.

10.5 Where there is a documented and approved business need to retain unsupported software, it shall only be installed on devices that are isolated from both internal company networks and external networks, including the internet. Such use shall be subject to a documented risk assessment and management approval.

11. Approval

11.1. This policy has been approved by the undersigned and will be reviewed at least annually.

Martyn Dixon

Managing Director 16th July 2026

Change information	
Document Change Number	CN0001
Description of Change	New Format for QM added to Policy
Reason for Change	Review and update the policy every 3 years, to bring the policy in line with QMS documentation.

Approval and Signatures of quality reviews			
Name	Role	Workflow	Decision
Patsy Stone	Author	13/11/2024	Approved
Patsy Stone	Revision	13/11/2024	Approved
Lara Peat	Reviewed	15/11/2024	Approved
Lara Peat	Approved	15/11/2024	Approved
Patsy Stone	Reviewed	22/04/2026	Approved
Cara Dixon	Revision	15/07/2026	Approved