Data Protection Policy

1. Introduction
   1.1. This Data Protection Policy is the overarching policy for data security and protection for Manchester Care and Repair.

2. Purpose
   2.1. The purpose of the Data Protection Policy is to support the 7 Caldicott Principles, 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

      2.2.1. Our data protection principles and commitment to common law and legislative compliance;

      2.2.2. 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 the services we provide to them. 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 Management 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.

4.8. 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 every individual's 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 the Data Protection Champion role. The Data Protection Champion will report to the highest management level of the organisation. We will support the Data Protection Champion with the necessary resources to carry out their tasks and ensure that they can maintain expertise.

5. Underpinning policies & procedures

5.1. This policy is underpinned by the following:

5.1.1. Record Management 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;

5.1.2. Data and Network Security Policy – outlines procedures for the ensuring the security of data including the reporting of any data security breach;

5.1.3. 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;

5.1.4. Confidentiality Policy - provides staff with clear guidance on the disclosure of personal information.

6. Data protection by design & by default

6.1. 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.

6.2. 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.

6.3. We will consider carrying out a Data Processing Impact Assessment prior to commencing any major project involving the use of personal data.

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

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

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

6.7. 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.

6.8. Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our clients and our staff.

7. Responsibilities

7.1. Our designated Data Protection Champion is The Corporate Resources Manager. The key responsibilities of the lead are:

7.1.1. 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;

7.1.2. 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.

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

7.1.4. To monitor information handling to ensure compliance with law, guidance and the organisation's procedures and liaising with the Senior Information Risk Owner (SIRO) to fulfil this work.

7.2. Our Senior Information Risk Owner (SIRO) is the Executive Director The key responsibilities of the SIRO are:

7.2.1. To manage, assess and mitigate the information risks within our organisation;

7.2.2. To represent all aspects of information and data protection and security to the Trustees and drive engagement in data protection at the highest levels of the organisation.

8. Approval

8.1. This policy draft has been approved by the undersigned and will be reviewed at least bi-annually. It replaces our previous data security policy to be in line with the NHS DPST

The 10 data security standards

Standard #	Application
1	All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form.
2	All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
3	All staff complete appropriate annual data security training and pass a mandatory test.
4	Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
5	Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
6	Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
7	A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.
8	No unsupported operating systems, software or internet browsers are used within the IT estate.
9	A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
10	IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.