Data and Network Security Policy

1. Introduction

1.1. This Data and Network Security Policy is Manchester Care and Repair's policy regarding the safeguarding and protection of sensitive personal information and confidential information as is required by law (including, but not limited to, the Data Protection Act 2018, Health & Social Care Act 2012, and the Common Law duty of confidentiality).

2. Purpose

2.1. The purpose of this document is to outline how we prevent data security breaches and how we react to them when prevention is not possible. By data breach we mean a security incident in which the confidentiality, integrity or availability of data is compromised. A breach can either be purposeful or accidental.

2.2. This Data and Network Security Policy covers:

- Physical and digital data access procedures;
- Data Security Audit Procedures;
- Data security breach procedures.
- IT and Network security policy

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. Physical and Digital Access Procedures

4.1. The Information Asset Register (IAR) will contain the location of all confidential and sensitive personal information.

4.2. Our staff must keep personal and confidential data securely in locked filing cabinets in our offices at Empress Business Centre, keys should not be left in the barrels of filing cabinets and doors and the offices, when left

unoccupied, must be locked**.** Digital records must be kept in the appropriate folders and drives within the digital filing system.

4.3. Physical and digital access to records shall only be granted on a 'Need to Know' basis. Staff who requires access to digital systems for their job role will be trained on the use of the system, given their user login details, and they will be required to sign to indicate that they understand the conditions of access. Digital records must only be accessed using a personal login.

4.4. During their induction each staff member who requires access to confidential information for their job role will be shown how this data is used, stored, shared and organised in our organisation. This applies to both physical and digital records.

4.5. Any changes to user access requirements must be authorised by the Data Protection Champion. A record of who has access to which records will be kept by the HR administrator.

4.6. As soon as an employee leaves, the Data Protection Champion will ensure that their system logons are revoked.

5. Data Security Audit Procedures

5.1 An audit will be completed at least annually to ensure that;

- Confidential information is secured properly
- Allocation of access rights to confidential information is appropriate.
- Any lapsed or unwanted logons are deleted
- The Information Asset Register has been reviewed, updated and signed off
- The Record of Processing Activities has been reviewed, updated and signed off
- Any confidentiality incidents or data breaches have been reviewed and appropriate actions have been taken
- Staff are aware of policies and guidelines concerning confidentiality and understanding of their responsibilities with regard to confidentiality;
- Communications with service users clearly reference data protection and consent forms/verbal consents are appropriately worded and recorded.

- Correct processes are used to securely transfer personal information in person, by post, by email or by other electronic means and that appropriate data transfer and sharing arrangements are in place
- Appropriate security is applied to PCs, laptops and mobile electronic devices
- The records retention schedule is reviewed and any disposals of confidential waste are made securely.

6. Data Security Breach Procedures

6.1. In order to mitigate the risks of a security breach we will:

- Follow the Physical and Digital Access and Data Security Procedures;
- Ensure our staff are trained to recognise a potential data breach;
- Ensure our staff understand the procedures to follow and how to escalate a data security incident to the correct person

6.2. If it appears that a data security breach has taken place:

- The staff member who notices the breach will inform the Executive Director immediately or, if they are not available, a member of senior management.
- The Executive Director will conduct an investigation into the potential breach.

6.3. If a personal data breach is identified – and if it is likely that there will be a risk to the rights and freedoms of an individual then the Information Commissioner's Office (ICO) will be informed as soon as possible, but at least within 72 hours of our discovery of the breach, via the DSPT Incident Reporting Tool (www.dsptoolkit.nhs.uk/incidents/); As part of any report we will provide the ICO with the following details:

- The nature of the personal data breach (i.e. confidentiality, integrity, availability);
- The approximate number of individuals concerned and the category of individual (e.g. employees, mailing lists, service users);
- The categories and approximate number of personal data records concerned;
- The name and details of our Data Protection Champion

- The likely consequences of the breach
- A description of the measures taken, or which we will take, to mitigate any possible adverse effects.

6.3.1. The Data Protection Champion will inform any individual that their personal data has been breached if it is likely that there is a high risk to their rights and freedoms. We will inform them directly and without any undue delay;

6.4. A record of all personal data breaches will be kept including those breaches which the ICO were not required to be notified about.

7. IT Infrastructure and Network Security

1.1. IT infrastructure and network management is outsourced to contractors. ***The contractors are*** responsible for ensuring that;

- The network does not pose an unacceptable security risk to the organisation. measures are in place to detect and protect the network from viruses and other malicious software, attacks are reported regularly
- any actual or potential data breach is reported immediately to the Executive Director
- effective data backup procedures and recovery plans are in place
- Physical IT infrastructure is appropriately protected from tampering, power outages etc.
- ensuring that where equipment is being disposed of all data on the equipment (*e.g.* on hard disks or tapes) is securely overwritten

1.2 The Executive Director and the Corporate Resources Manager are responsible for periodically reviewing the type and level of service provided and the performance of contractors.

1.3 The Executive Director is responsible for ensuring

2. Responsibilities

2.1. **The Data Champion (Corporate Resources Manager) is responsible** for physical security and digital access and for staff training and induction

2.2. **The Executive Director** is responsible for updating the IAR and ROPA, for data security audits and for managing breaches.

2.3. The IT contractors are responsible for updating all relevant Network Security Policies, design documentation, security operating procedures and network operating procedures.

3. Approval

3.1. This **draft** policy replaces our previous GDPR policy in line with the requirements of the NHS Data Protection and Security Toolkit. It has been approved by the undersigned and will be reviewed at least bi-annually.

Appendix: Data Security Audit Checklist

Staff	**Responsible**	**Date audited**
Check that staff understand their responsibility towards data security and are aware of our data protection polices	LN	
All staff have received training on data protection?	LN	
Check that staff understand how to report security breaches	LN	
Physical Access to hardcopy records		
Update record of which staff have access to confidential paper records	LN	
All offices, files, or cabinets which contain confidential information are kept locked when not in use.	LN	
Check retention record and ensure confidential waste is disposed of securely and has a destruction certificate	LN/AMt	
Digital Access to records		
Review staff access rights and delete defunct log ins	AMt/IT	
Have appropriate security measures been applied to all computers, laptops and mobile devices?	AMt/IT	
Sharing data		
Our procedures for safely sharing personal information by hand and by post are being followed.	LN/AMt LN/AMt	
Our procedures for safely sharing personal information via secure email are being followed.		
Legal Checks		
The Information Asset Register has been reviewed and signed off.	AM	
The Record of Processing Activities has been reviewed and signed off.	AM	
Records of consent are up to date and still applicable.	AM	
IT infrastructure and Network		
The IT contractors SLA have been reviewed and amended as required With particular reference to security	AM/AMt	
Backup and restore and business continuity plans have been reviewed and updates as appropriate	AM/AMt	