# Network Security Policy

## **Introduction**

* 1. This Network Security Policy is the overarching policy for data security and protection for Castlehead Medical Centre (hereafter referred to as "us", "we", or "our").

## **Purpose**

* 1. This document sets out our policy for the protection of the confidentiality, integrity and availability of the network, establishes responsibilities for network security and provides reference to documentation relevant to this policy.

## **Scope**

* 1. This policy applies to all staff, including temporary staff and contractors.
	2. This policy applies to ournetworks which are used for:
		1. The storage, sharing and transmission of non-clinical data and images;
		2. The storage, sharing and transmission of clinical data and images;
		3. Printing or scanning non-clinical or clinical data or images;
		4. The provision of internet systems for receiving, sending and storing non-clinical or clinical data or images.

## Policy

* 1. Castlehead Medical Centre’s information network will be available when needed, can be accessed only by legitimate users and will contain complete and accurate information.
	2. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality. To satisfy this we undertake to:
		1. Protect all hardware, software and information assets under its control;
		2. Provide effective protection that is commensurate with the risks to its network assets;
		3. Implement the Network Security Policy in a consistent and timely manner;
		4. To comply with all relevant legislation.

## **Risk assessments**

* 1. We will carry out security risk assessment(s) in relation to all the business processes covered by this policy. These risk assessments will cover all aspects of the network that are used to support those business processes.
	2. The risk assessment (our data audit policy) will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

## **Physical & environmental security**

* 1. Critical or sensitive network equipment will be housed in secure areas.
	2. Critical or sensitive network equipment will be protected from power supply failures.
	3. Critical or sensitive network equipment will be protected by intruder alarms and fire suppression systems.
	4. Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.
	5. All visitors to secure network areas must be logged in and out. The log will contain name, organisation, purpose of visit, date, and time in and out.
	6. The Practice Manager and Reception Managerwill ensure that all relevant staff are made aware of procedures for visitors and that visitors are escorted, when necessary.

## **Access control to the network**

* 1. Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access. Remote access to the network will be allowed using approved equipment.
	2. Third party access to the network will be based on a formal written contract.
	3. All third-party access to the network must be logged.

## **External network connections**

* 1. We will ensure that all connections to external networks and systems have documented and approved System Security Policies.
	2. North Cumbria Integrated Care NHS Foundation Trustmust approve all connections to external networks and systems before they commence operation.

## **Maintenance contracts**

* 1. The Practice Managerwill ensure that maintenance contracts are maintained and periodically reviewed for all network equipment.
	2. All contract details will constitute part of the Information Asset register (IAR).

## **Data & software exchange**

* 1. Formal agreements for the exchange of data and software between organisations must be established and approved bythe practice manager/IT lead.
	2. All exchanges of data between organisations will be recorded on the Record of Processing Activities (ROPA).

## **Fault logging**

* 1. The practice manager/IT manager are responsible for ensuring that a log of all faults on the network is maintained and reviewed. A written procedure to report faults and review countermeasures can be located on TeamNet.

## **Security operating procedures & Network operating procedures**

* 1. See standard operating procedures on TeamNet
	2. Changes to operating procedures must be authorised by the relevant managers.

## **Data backup & restoration**

* 1. Data backup procedures are outlined in the Emergency and Business Continuity Plan document.

## **User responsibilities, awareness & training**

* 1. Wewill ensure that all users of the network are provided with the necessary security guidance, awareness and training to discharge their security responsibilities.
	2. These procedures will be outlined in the staff handbook.

## **Accreditation of network systems**

* 1. The Practice Manageris responsible for ensuring that the network does not pose an unacceptable security risk to the organisation. They will require checks on, or an audit of, actual implementations based on approved security policies.

## **Malicious software**

* 1. We will ensure that measures are in place to detect and protect the network from viruses and other malicious software.

## **Secure disposal or re-use of equipment**

* 1. We will ensure that where equipment is being disposed of all data on the equipment (*e.g.* on hard disks or tapes) is securely overwritten.

## **System change control**

* 1. The Practice Manager and Data Protection Championisresponsible for updating all relevant Network Security Policies, design documentation, security operating procedures and network operating procedures.

## **Reporting security incidents & weaknesses**

* 1. All potential security breaches must be reported to the NCIC IT Security Team by email: suspect-emails@cumbria.nhs.uk or if there is an immediate data security risk call 01228 608888
	2. We will follow the procedures set out in the Data Security Policy.

## **Business continuity & disaster recovery plans**

* 1. We will ensure that business continuity plans are produced for the network.
	2. The plans must be reviewed and tested on a regular basis.

## **Approval**

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

|  |  |
| --- | --- |
| Name | Laura Dakers & Carole Bell |
| Signature | Laura Dakers |
| Approval Date | 02.06.21 |
| Review Date | 01.04.21 |