QMSIT05 Information Security Policy

VERSION:	12
DATE LAST UPDATED:	March 2021
REVIEW DATE:	March 2022
RELATED DOCUMENTS:	
OWNER / LEAD INDIVIDUAL:	**Lead Individual:** Chief Executive Officer (CEO)
DOCUMENT APPROVAL:	**Peer/Subgroup:** Systems Oversight group
PATIENT ACCESS:	☺
SECURITY INFORMATION (PUBLIC, INTERNAL, CONFIDENTIAL):	Public

Version Control Sheet

Policy Name:	Information Security Policy	Policy Reference:	QMSIT05

Version	Date	Comment
01	Jan-14	New Policy
02	Jan-15	Annual review, Information Security Management Group included
03	Feb-15	Addition of Clear Desk and Clear Screen Policy, as well as Use and Installation of Software, Backup and Network and Infrastructure
04	Feb-15	Replaced all "should" statements with "shall" following risk assessment
05	May-15	Inclusion of procedure of approval if urgent removable media access is required
06	May-16	Annual Review, reviewed as a part of desktop audit, new Lead Individual due to changes in the hospital's structure, Peer/Subgroup IG/ISM added
07	June-2017	Annual Review, no changes made
08	Jan 2018	Update of key titles due to organisational change
09	May 2018	Reviewed and updated in line with the Data Protection Act 2018/ General Data Protection Regulation
10	May 2019	Annual Review
11	August 2020	Annual Review, minor changes throughout
12	March 21	Full review to meet all ISO27001 requirements

Preface

Cheswold Park Hospital (CPH) recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. Information governance plays a key part in the delivery of clinical governance, service planning and performance management.

To protect the confidentiality, integrity and availability of our information, Cheswold Park Hospital have approved and implemented an information security management system built on the ISO 27001:2013 standard.
It identifies, manages and minimizes the range of threats to which information can be subjected. The standard is designed to ensure the implementation of adequate and proportionate security controls that protect Cheswold Park Hospital's assets and give confidence to interested parties including regulators and our patients.

Cheswold Park Hospital is committed to ensure that:

- All information will be protected from unauthorised access or disclosure (confidentiality).
- All information will be protected from accidental, malicious and fraudulent alteration or destruction. Information will be complete and accurate (integrity).
- Information will be consistently and readily accessible for authorised parties (availability).

This Information Security Policy shall therefore be considered as a key aspect of an overarching framework for the local delivery of Information Governance at Cheswold Park Hospital. This policy confirms Cheswold Park Hospital's commitment to continuous improvement of its information security management system.
The Chief Executive Officer (CEO) approves this policy. This information security policy shall be communicated within the organisation and available to all interested parties. Information Security Policies are located in our intranet (QMS) under Information Governance / IT sections.

1 Scope

Cheswold Park Hospital provides services & therapies for people diagnosed with Personality Disorder, Mental Illness and Intellectual Disabilities. The Information Security Management System offers protection to all information processed and stored within Cheswold Park Hospital in course of providing those services. ISMS covers all employees (part-time, full-time, temporary staff, consultants, contractors and vendors)and systems employed within Cheswold Park Hospital with a geographical location as below:

Cheswold Park Hospital
Cheswold Lane

Doncaster
DN5 8AR

2 Responsibilities and commitment

The Executive Leadership Team is committed to satisfy all requirements within this policy and to the continuous improvement of the ISMS.

Top management will continue to demonstrate commitment with respect to the information security management system by:

- ensuring the integration of the information security management system requirements into the organisation's processes;
- ensuring the information security policy and information security objectives are established;
- communicating the importance of the information security management system;
- ensuring that the resources needed for the information security management system are available;
- promoting continual improvement.

The Chief Executive Officer (CEO) has overall accountability and responsibility for Information Governance which includes Information Security.

Caldicott Guardians have a responsibility to ensure patient data is kept secure. The Hospital's Caldicott Guardian is the Medical Director.

The Senior Information Risk Owner (SIRO) acts as an advocate for information risk within the Hospital and has responsibility for the ongoing development of the Hospital's Risk Management programme for Information Governance and Security.

3 Legislation

The Hospital is obliged to abide by all relevant legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the Hospital, who may be held personally accountable for any breaches of information security for which they may be held responsible. The Hospital shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (2018)
- EU GDPR 2016/679
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)

- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000

4 Information Security Objectives

The key objective is to work in line with the sections of the best practice standard ISO 27001:2013 to enhance stakeholders' confidence and to safeguard confidential information.

Furthermore, security objectives will be set by management as an ongoing task and at ISMS management Review Meetings (Hospital Governance meetings, Systems Oversight Committee meetings). Objectives for Information Security will be continually monitored to ensure they are achieved.

5 Controls and security across different areas

5.1 Access Controls

Employees must be aware of and must follow a number of controls and procedures, which exists to limit access to information.
All staff will be issued with an individual computer login. This will include a username and password. This will provide access to an individual e-mail account. The log in shall be used on any PC within the hospital and enable access to appropriate information and shared drives. Access is dependent on the user, please see QMSIT01 Computer Acceptable Use Policy for details on Access Management and QMSIT06 Information Security Controls more details.

5.2 Internet Controls and Access Policies

The internet use of all staff is monitored and managed by the Web Monitoring software. The default policy will be to block web sites categorised as offensive or inappropriate.

All internet use is logged and reports are produced monthly for management and monitoring purposes. The Hospital reserves the right to monitor activity in general and where it suspects that there has been a breach of policy.

5.3 Clear Desk and Clear Screen Policy

To improve security and the confidentiality of Information, Cheswold Park Hospital has adopted a clear desk policy for papers and a clear screen policy for information processing facilities. This is to reduce the risk of unauthorised access, loss of and damage to information when areas are unattended.

The Clear Desk and Clear Screen policy will be regularly monitored with spot checks carried out.

5.4 Cryptographic Controls

Cheswold Park Hospital's information system resources shall be appropriately protected to prevent unauthorised access by applying a level of encryption to sensitive or personal identifiable information. Please see section 5.7 of the QMSIT01 Computer Acceptable Use Policy for the use of encrypted removable media.

5.5 Physical and Environmental Security

Staff must be aware of and must follow the detailed set of measures, controls and procedures that exist to ensure adequate control of physical security. These include:

- restricted access to the building and within it,
- electronic fobs and locking systems,
- alarm system,
- cctv system,
- secure offsite backups

Please see QMSSO01 Physical Security Document for details.

5.6 Communication security

Cheswold Park Hospital is heavily reliant on the IT Network Infrastructure to provide effective healthcare to its service users, therefore it is essential that this vital resource is maintained to a high level to ensure service continuity and security of its information assets and supporting business processes. Along with ensuring security and compliance, this policy is also a key requirement in guaranteeing the Hospital's obligations are met in relation to the Information Security.

5.7 Human Resources Security

All employees must be trained on procedures as part of their induction programme. Internal Information Governance and external Data Security awareness trainings are included within this induction. Confidentiality of information section is included in all staff contracts (section 15).

5.8 Supplier Relationship

Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets must be agreed and documented. Please see QMSQU07 Approved Suppliers Procedure for details.

6 Data Breach and Information security Events and Weaknesses

All information security events and suspected weaknesses are to be reported in line with the Hospital's Data Breach Response and Notification Procedure (QMSIG10). For further advice or guidance and where it is suspected that a Caldicott breach (patient identifiable data breach) may have taken place the Caldicott Guardian / Quality and Data Protection Officer shall informed as soon as is practicable.

7 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

8 Management Reviews and Reporting

The Systems Oversight group keep the Leadership Team informed of the information security status of the Hospital.

When reviewing ISMS, Management's responsibilities include:

- Assessing results of ISMS audits and reviews;
- Checking status of preventive and corrective actions;
- Assessing vulnerabilities or threats
- Reporting on results from effectiveness measurements;
- Following-up on actions from previous management reviews;
- Checking on any changes that could affect the ISMS; and
- Providing recommendations for improvement.

Regular Management Reviews should result in the following:

- Improvement of the effectiveness of the ISMS.
- Update of the risk assessment and risk treatment plan.
- Modification of procedures and controls that effect information security.
- Responding to internal or external events that may impact on the ISMS.

IMPACT EQUALITY ASSESSMENT

Cheswold Park Hospital is committed to ensuring that as far as is reasonably practicable, the way we provide services for our patients, visitors and treat our staff reflects their individual needs and does not discriminate against individuals or groups on any grounds.

1. Screening			
How relevant is this policy and its associated procedures to promoting equality and eliminating discrimination? (indicate in boxes below)			
	Not relevant	Partly relevant (state which parts)	Very relevant
Race/ethnic group	✓		
Disability[1]	✓		
Gender	✓		
Age	✓		
Sexual Orientation	✓		
Religion	✓		
Other (please state)			
2. Assessing Impact (to be completed where the policy and associated procedures has been determined as relevant in the screening process)			
Please specify, in the rows below, anything that you have included in this policy and its associated procedures to ensure that equality is promoted and that no-one will be unlawfully disadvantaged (discriminated against) as a result of this policy.			
Race/ethnic group			
Disability[1]			
Gender			
Age			
Sexual Orientation			
Religion			
Other (please state)			

[1] Disability covers physical, sensory and mental impairments which include mental illness and learning disability. Long term conditions such as cancer, HIV and Multiple Sclerosis are included and any other normal condition at the point at which it begins to have an impact on a person's capacity to carry out normal day to day activities.