Walsall Healthcare NHS
NHS Trust

Document Title
Information Security & Access Control Policy

Document Description	
Document Type	Policy
Service Application	Trust Wide
Version	2.0

Lead Author(s)	
Name	Job Title
Nigel Malone	Infrastructure Service Manager
Sharon Thomas	Corporate Governance Manager

Executive Director / Director / Manager			
If you are assured that the correct procedure has been followed for the consultation of this policy, sign and date below:			
Name	Director of Strategy and Improvement	Date	
Signature		01.04.2019	

Change History		
Version	Date	Comments
1.0	13/11/17	Initial draft
1.2	9/5/18	Updated draft
2.0	1/2/2019	Updated in line with GDPR and Toolkit

Links with External Standards	
Network & Information Systems Directive 2017	
Data Protection Act 1998 General Data Protection Regulations 2017	
Computer Misuse Act 1990	
Investigatory Powers Act 2016	
Data Retention & Investigatory Powers Act 2014	

Key Dates	DATE
Ratification Date	26th March 2019 by TMB
Review Date	Feb 2021

Executive Summary Sheet

Document Title:	**Information Security & Access Control Policy**	
Please Tick (☑) as appropriate	This is a new document within the Trust	☑
	This is a revised Document within the Trust	

What is the purpose of this document?

To provide a balance between security and ease of use by providing a comprehensive and consistent approach to the security management of digital information across the Trust in line with the Department of Health Information Security Management NHS Code of Practice (April 2007)

What key Issues does this document explore?

This policy provides a comprehensive and consistent approach to the security management of information across the Trust. It will ensure continuous business capability, and minimise both the likelihood of occurrence and the impacts of any information security incidents.

Who is this document aimed at?

All staff working for Walsall Healthcare NHS Trust

What other policies, guidance and directives should this document be read in conjunction with?

IM&T policy
WITS IT Security SOP
NHS Digital Standards
NHS Digital guidance for IT Systems in health & care settings
RA Policy
Disciplinary Policy
Raising Concerns at Work (Whistleblowing) Policy
Acceptable Use Guidelines
Anti-Virus & Malware Guidelines
Network & Information Systems Regulations 2017
The Data Protection Act (GDPR) 2018
Computer Misuse Act 1990
Information Governance and Management Strategy
General Data Protection Regulations Policy and Procedures

How and when will this document be reviewed?
At least every three years by the lead author or by an individual nominated by the lead Director.

CONTRIBUTION LIST

Key individuals involved in developing the document

Name	Designation
	Infrastructure Service Manager
	IT Service Delivery Manager
	Assistant Director IT Services
	Infrastructure Support Manager
	Corporate Governance Manager

Circulated to the following for consultation

Name/Committee/Group/	Designation
Intranet Forum	
Policies and Procedures Members	
Director of Strategy and Improvement	Director of Strategy & Improvement & SIRO
Threat Assessment Group (TAG)	
Information Governance Steering Group (IGSG)	
Informatics Operational Group (IOG)	
Human Resource Management Group	

Version Control Summary

Significant or Substantive Changes from Previous Version

A new version number will be allocated for every review even if the review brought about no changes. This will ensure that the process of reviewing the document has been tracked. The comments on changes should summarise the main areas/reasons for change.

When a document is reviewed the changes should be recorded using the tracking tool below in order to clearly show areas of change for the consultation process.

Version	Date	Comments on Changes	Author
0.1	13/11/17	Initial draft	
1.2	09/05/18	Updated draft	
1.3	20/6/18	Updated draft	
2.0	01/02/19	Complete review following introduction of GDPR and best practice exercise	Corporate Governance Manager

INFORMATION SECURITY & ACCESS CONTROL POLICY

1.0 INTRODUCTION

The Information Security Policy outlines the approach, methodology and responsibilities for preserving the confidentiality, integrity and availability of the organisation's information. It is the overarching policy for information security and supported by specific technical security, operational security and security management procedures.

2.0 Purpose of Policy

The purpose of this Information Security and Access Control Policy and its associated documents is to ensure Walsall Healthcare NHS Trust has an overall digital information security management framework; to protect, to a consistently high standard, all Trust digital information assets, including patient records and other NHS corporate information from all potentially damaging threats, whether internal or external, deliberate or accidental.

All users of Trust IT systems must abide by the rules set out in this document. Users will be held personally responsible for failure to comply with the policy and may be subject to disciplinary action.

3.0 Statement of Intent

The trust is obliged to abide by all relevant UK and European Union legislation. The requirements to comply with this legislation shall be devolved to employees and agents of the Trust, who may be held personally accountable for any breaches of information security; failure to comply could result in the individual or the Trust being prosecuted. The Trust shall comply with the legislation, detailed in this document, and other legislation as appropriate.

4.0 Scope and limitations

This policy applies to all areas and activities of the Trust, including system accounts, and to all individual users employed by the Trust including contractors, volunteers, students, locum and agency staff, staff employed on honorary contracts, non-executive directors and any other individual or organisation granted access to Trust systems. This policy applies to all information held on electronic assets, including Trust information in transit and activities carried out on mobile devices.

4.1 OBJECTIVES

The objectives of this policy are to preserve:
Confidentiality – access to data is confined to those who have legitimate authority to view it.
Integrity – data is timely and accurate and detected or amended only by those specifically authorised to do so.
Availability – information shall be available and delivered to the right person, at the time when it is needed.

5.0 ROLES AND RESPONSIBILTIES

5.1 Members of the Information Governance Steering Group (IGSG)

The Information Governance Steering Group comprises the Trust's SIRO, Information Governance Manager, IT Manager, divisional representatives as well as representatives from Informatics and Medical Records. Through this group, the Board is advised of common approaches to information governance/security and assured of Trust practices.

5.2 Caldicott Guardian

The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles and Data Security Standards with respect to Patient Confidential Data.

The aim of the Caldicott Guardian is to ensure the organisation implements the Caldicott principles and data security standards.

5.3 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is accountable for information risk within Walsall Healthcare NHS Trust and advises the Board on the effectiveness of information risk management across the organisation. Operational responsibility for Information Security shall be delegated by the SIRO to the Assistant Director of IT Services and the TAG.

5.4 IT Security Management Team

The Threat Assessment Group (TAG) is responsible for the day to day operational effectiveness of the Information Security Policy and its associated policies and processes. The TAG shall:

(i) Lead on the provision of expert advice to the organisation on all matters concerning information security, compliance with policies, setting standards and ensuring best practice.

(ii) Provide a central point of contact for information security.

(iii) Ensure the operational effectiveness of security controls and processes.
(iv) Monitor and co-ordinate the operation of the Information Security Management System.

(v) Be accountable to the SIRO and other bodies for Information Security across Walsall Healthcare NHS Trust.

(vi) Monitor potential and actual security breaches with appropriate expert security resource.

5.5 Information Asset Owners/Local Record or Senior Managers

The aim of the IAO role is to have a nominated role or person to be responsible for the management and control of information assets.

The Information Asset Owners (IAOs) are senior/responsible individuals involved in running the business area and shall be responsible for:

(i) Understanding what information is held.
(ii) Knowing what is added and what is removed.
(iii) Understanding how information is moved.
(iv) Knowing who has access and why.

5.6 All Staff (with individual responsibilities under the policy)

Information Security and the appropriate protection of information assets is the responsibility of all users and individuals are expected at all times to act in a professional and responsible manner whilst conducting Walsall Healthcare NHS Trust business. All staff members are responsible for information security and remain accountable for their actions in relation to NHS and other UK Government information and information systems. Staff shall ensure that they understand their role and responsibilities, and that failure to comply with this policy may result in disciplinary action. This will be reinforced by yearly mandatory training.

5.7 Data Protection Officer

The Data Protection Officer is responsible for ensuring that Walsall Healthcare NHS Trust and its constituent business areas remain compliant at all times with Data Protection, Privacy & Electronic Communications Regulations, Freedom of Information Act and the Environmental Information Regulations. The Data Protection Officer shall:

(i) Lead on the provision of expert advice to the organisation on all matters concerning the Data Protection Act, compliance, best practice and setting and maintaining standards.

(ii) Provide a central point of contact for the Act both internally and with external stakeholders (including the Office of the Information Commissioner).

(iii) Communicate and promote awareness of the Act across the organisation.

(iv) Lead on matters concerning individual’s right to access information held by Walsall Healthcare NHS Trust and the transparency agenda.

5.8 Assistant Director of IT Services

The Assistant Director of IT has been delegated with responsibility for information security on behalf of the executive lead for IT for the Trust. The day to day activities required to effectively implement and maintain this policy will be performed through the IT Business Manager.

6.0 PROCEDURE

This policy sets out the high level framework for Information Security within the Trust.

In conjunction with information governance and data security principles, the aim of this policy is to establish and maintain the security and confidentiality of information within digital information systems, applications and networks owned or held by the Trust, by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and associated policies and procedures, through auditing, monitoring and reporting.

- Introducing a consistent approach to information security, ensuring that all members of staff fully understand their own responsibilities.

- Describing the principles of information security and explaining how they shall be implemented in the Trust.

- Creating and maintaining within the Trust a level of awareness of the need for information security as an integral part of the day to day business.

- Protecting information assets under the control of the Trust, to include any hosted or external applications.

- Ensuring staff do not remove information from the Trust unless approved to do so in consultation with Information Governance.

6.1 Contracts of Employment

Staff security requirements are addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause. Information security expectations of staff are including within appropriate job definitions.

6.2 Security Control of Assets

Each IT asset, (hardware, software, application or data; internally or externally supplied) shall have a named Information Asset Owner (IAO) who shall be responsible for the information security of that asset. IAOs can be assisted by one or more Information Asset Administrators (IAA). Information Governance maintains a copy of the asset register.

The flow of data between an IAO's assets and any internal or external systems or parties shall be included in the asset register.

Agreements with suppliers shall include requirements to address information security risks.

6.3 Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted services, or areas containing information systems or stored data. Exceptional access privileges will only be given with approval from the Senior

Information Risk Owner (SIRO).

6.4 User Access Controls

Access to information shall be restricted to authorised users who have a legitimate business need to access the information and in accordance with the principle of least privilege.

6.5 Computer Access Controls

Access to computer facilities shall be restricted to authorised users who have a business need to use the facilities.

6.6 Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

6.7 Digital Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. This will be achieved by the effective use of suitable security measures i.e. physical controls within buildings, entry systems and secure storage facilities to protect assets from theft/damage.

6.8 Computer and Network

Management of computers shall be controlled through standard documented procedures that have been authorised by the Trust.

IT schedules back-ups on business critical databases and network files to enable recovery. Off-line, network disconnected copies shall be kept in addition to network accessible copies.

Trust digital equipment must not be used for private work, commercial activities, advertising or fundraising if not directly connected with the Trust, unless it has had formal Trust approval.

Network integrity shall be protected through employing segregation and cryptographic techniques where appropriate.

6.9 Remote Access

Remote access to Trust network and systems shall be through software and services provided by the Trust which requires additional user authentication. Staff and third party suppliers using remote access facilities shall do so from private locations and using secure network connections.

Third party support access will be provided by IT Services, via accounts providing the least privilege necessary to perform the required duties for the shortest amount of time.

Staff shall ensure that computers used for remote access are using up to date malicious software (‘malware’) protection. Any personally identifiable data (PID) or Trust intellectual property accessed from remote locations shall not be stored locally.

Staff will ensure that family and friends do not have access to trust services and systems at the remote location. Staff will be aware of their surroundings when using mobile devices in public places so that members of the public or relatives do not view personal information.

6.10 Information Risk Assessment

The principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

Once identified, information security risks shall be managed on a formal basis by their IAO in line with Risk Management Strategy and Policy. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

The NHS Digital good practice guides, National Cyber Security Centre (NCSC) 10 steps to Cyber Security, NCSC Cyber Essentials assurance framework and ISO 27001 Information Security Management Standard will be considered when risk assessing information security risks.

6.11 Information Security Events and Weaknesses

All information security events and suspected weaknesses are to be reported to the IT Service Desk. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events. Incidents and near misses will be reported in line with the Trusts Reporting and Management of Incidents, including serious incidents, policy. External event reporting will be in agreement between Information Governance and Information Technology departments.

The primary goal of handling an information security incident shall be to resume the normal security level, followed by the necessary recovery and corrective actions. Information security threat and vulnerability information is to be received and actively sought from a variety of authoritative and special interest information sharing sources.

Serious events that require forensic investigation will do so in accordance with the NHS Digital Forensic Readiness Good Practice Guide.

Reporting must happen as soon as the event is discovered.

Software and hardware shall be maintained through its lifetime with the implementation of updates and alternatives (‘patches’).

6.12 Protection from Malware

The Trust shall use software countermeasures and management procedures to protect itself against the threat of malware. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the Trusts property without permission from the Trust; any such requirements must be raised with the IT Service Desk, by logging a call. Users breaching this requirement may be subject to disciplinary action. The Trust shall undertake scans for vulnerabilities from malware.

6.13 User Media

Removable media of all types that contain software or data from external sources, or that have been used on external digital equipment, require the approval of the Trust before they may be used on Trust systems. Read only access to removable media is permitted, provided such media is fully virus checked before being used on the Trusts equipment. Users breaching this requirement may be subject to disciplinary action.

6.14 Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis; in so far as is practically possible, subject to technical limitations. The scope and retention of audit trail data shall be sufficient to support retrospective analysis of individuals’ activities.

The Trust has in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees’ electronic communications (including telephone communications) for the following reasons:

- establishing the existence of facts;
- investigating or detecting unauthorised use of the system;
- preventing or detecting crime;
- ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training);
- in the interests of national security;
- ascertaining compliance with regulatory or self-regulatory practices or procedures.
- ensuring the effective operation of the system

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act.

6.15 Accreditation of Information systems

The Trust shall ensure that all new information systems, applications and networks include an approved security plan before they commence operation.

IAOs are responsible for carrying out Impact Assessments, annual risk assessments/reviews for systems under their control.

6.16 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Trust. IT changes are subject to the completion and approval of the 'Request for Change' form. System developments shall follow a defined life cycle.

6.17 Intellectual Property Rights

The Trust shall ensure that all digital information products are properly licenced and approved by the Trust. The Trust will take appropriate steps to protect its intellectual property rights to any locally developed systems and will protect that right accordingly.

6.18 Business Continuity & Disaster Recovery Plans

The Trust shall ensure that business impact assessments, business continuity and disaster recovery plans are produced, tested and deployed when necessary for all mission critical digital information, applications, systems and networks.

6.19 Digital Equipment Disposal

NHS and third party systems which deal with personal identifiable data (PID), confidential or sensitive information will be disposed of in line with national requirements to prevent unauthorised disclosure.

All redundant equipment must be disposed of in line with:

- NHS Digital disposal and Destruction of Sensitive Data
- The Information Commissioner's Office (ICO) IT asset disposal for organisations
- The Waste Electronic and Electrical Equipment Directive (WEEE)

7.0 EQUALITY IMPACT ASSESSMENT

The users of this policy will take into account their statutory duty to promote equality and human rights and to act lawfully within current equality legislation and guidance.

This policy has been equality impact assessed and has been shown to have no adverse impact on any equality group.

The Trust will continue to monitor its effect and will assess again if negative impact is identified or at the review date.

7.1 Financial implications

Any financial implications will be considered as part of the annual budget setting process across the Trust.

7.2 Risk Implications / Risk Assessment

There are no risk implications associated with this policy subject to successful implementation and compliance. The implementation of this policy mitigates risk around inappropriate use of digital assets and the standards within the Information Governance Toolkit.

8.0 MONITORING, CONTROL AND AUDIT

Monitoring Process	**Requirements**
Who	The Threat Assessment Group (TAG)
Standards Monitored	• Audit of system access and data use by staff; • Trend analysis on system access; • Review of enhanced privileged access assignment to digital information assets; • Reports on lost or stolen mobile devices; • Reports on redundant mobile devices usage; • Monitoring of network activity.
When	Bi-annually
How	Audit
Presented to	Information Governance Steering Group
Monitored by	Information Governance Steering Group
Completion/Exception reported to	Quality and Safety Committee
Who	Information Governance Manager
Standards Monitored	Completion of mandatory data security and awareness training
When	Bi-annually
How	Audit
Presented to	Information Governance Steering Group
Monitored by	Information Governance Steering Group
Completion/Exception reported to	Quality and Safety Committee

Areas of non-conformance will be highlighted to the relevant departments and recommendations suggested to tighten controls or make adjustments to related procedures.

9.0 TRAINING

Information security awareness is included in the mandatory training. Ongoing information campaigns take place throughout the year to ensure that staff awareness is maintained.

Training is provided both face to face and via e-learning and this includes specific training for Information Asset Owners/Administrators.

10.0 DEFINITIONS

The following terms are used within this policy:

AV	Anti-virus
GDPR	General Data Protection Regulations
IAA	Information Asset Administrator
IAO	Information Asset Owner
IGSG	Information Governance Steering Group
IT	Information Technology
RMC	Risk Management Committee
SIRO	Senior Information Risk Owner
TAG	Threat Assessment Group. It consists of 4 members of IT Services: IT Business Manager, Infrastructure Services Manager, Infrastructure Support Manager, Server SME all of whom are based at Eldon Court.

11.0 BEST PRACTICE, EVIDENCE AND REFERENCES

- Freedom of Information Act 2000
- Health & Social Care (Safety & Quality) Act 2015
- Computer Misuse Act 1990
- Network and Information System Regulations (NIS) 2017
- The General Data Protection Regulations/ Data Protection Act 2018
- Human Rights Act 1998
- Information Security Management: NHS Code of Practice – DH 2007
- Information Security Code of Practice – DH
- NHS Digital Information Governance Toolkit
- Telecommunications (Lawful Business Practice) Interception of communications regulations 2000
- Risk Management Strategy & Policy/Procedures
- Information Governance Policy

Appendix 1

Checklist for the Review and Approval of Procedural Documents

To be completed and attached to any procedural document that requires ratification

	Title of document being reviewed:	Yes/No	Comments
1.	**Title**		Information Security & Access Control Policy
	Is the title clear and unambiguous? It should not start with the word policy.	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**	Yes	
	Are reasons for development of the document stated? This should be in the purpose section.	Yes	
3.	**Development Process**		
	Does the policy adhere to the Trust policy format?	Yes	
	Is the method described in brief? This should be in the introduction or purpose.	Yes	
	Are people involved in the development identified?	Yes	
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
	Are all terms clearly explained/defined?	Yes	
5.	**Evidence Base**		
	Has a comprehensive literature search been conducted to identify best evidence to inform the policy?	Yes	
	Have the literature search results been evaluated and key documents identified?	Yes	
	Have the key documents been critically appraised?	Yes	
	Are key documents cited within the policy?	Yes	
	Are cited documents referenced?	Yes	

6.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
	If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?	No	
	For Trust wide policies has the appropriate Executive lead approved the policy?	Yes	
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	Yes	
	Does the plan include the necessary training/support to ensure compliance?	Yes	
8.	**Document Control**		
	Does the document identify where it will be held?	Yes	
	Have archiving arrangements for superseded documents been addressed?	Yes	
9.	**Process to Monitor Compliance and Effectiveness**		
	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	Yes	
	Is there a plan to review or audit compliance with the document?	Yes	
10.	**Review Date**	Yes	
	Is the review date identified?	Yes	
	Is the frequency of review identified? If so is it acceptable?	Yes	
11.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the documentation?	Yes	

Reviewer			
If you are assured that the correct procedure has been followed for the consultation of this policy, sign and date			
Name		Date	January 2019
Signature		Approving Committee/s	TAG/IGSG/Policies and Procedures Group

Lead Manager (Local Policies) / Director (Trust Wide Policies)			
If you are assured that the correct procedure has been followed for the consultation of this policy, sign and date it and forward to the Compliance and Risk Department for ratification.			
Name		Date	
Signature		Approving Committee/s	TAG/IGSG/Policies and Procedures Group
Ratification Committee Approval			
Quality Board minute number: PPG minute number: **TMB minute number:**			

Appendix 2

Service Overview & Improvement Action Plan: Equality Analysis Form

Title: Information Security & Access Control Policy	What are the intended outcomes of this work? To provide a balance between security and ease of use by providing a comprehensive and consistent approach to the security management of digital information across the Trust in line with the Department of Health Information Security Management NHS Code of Practice (April 2007)
Who will be affected? All staff	Evidence: N/A

ANALYSIS SUMMARY: considering the above evidence, please summarise the impact of the work based on the Public Sector equality duty outcomes against the 9 Protected characteristics

Public Sector Duty *Protected Characteristics* (highlight as appropriate)	**Eliminate discrimination, harassment and victimisation**	**Advance equality of opportunity**	**Promote good relations between groups**
AGE / DISABILITY/ RACE	*No Impact*	*No Impact*	*No Impact*
SEX (Gender)/ GENDER REASSIGNMENT	*No Impact*	*No Impact*	*No Impact*
RELIGION or BELIEF/ SEXUAL ORIENTATION	*No Impact*	*No Impact*	*No Impact*
PREGNANCY & MATERNITY	*No Impact*	*No Impact*	*No Impact*
MARRIAGE & CIVIL PARTNERSHIP	*No impact*	*Not applicable at present*	*Not applicable at present*

What is the overall impact? There are no negative implications associated with this policy. The implementation promotes positive opportunities and relationships between all groups and is in accordance with the new General Data Protection Regulations.

Any action required on the impact on equalities? *Impact of this policy has been assessed and it will not lead to any discrimination or other adverse events on any population groups, as described above.*			
Name of person completing analysis	*Corporate Governance Manager*	**Date completed**	*January 2019*
Name of responsible Director	*Director of Strategy and Improvement*		
Signature			