SCW

NHS
South, Central and West
Commissioning Support Unit

OFFICIAL

Information Security Policy

Version 5.0 July 2023

Document control

Document name	Version	Status	Author
Information Security Policy	5.0	Final	Cyber Security Manager
Document objectives:	The objective of this Information Security Policy is to safeguard the confidentiality, integrity and availability of information, information systems, applications and networks owned or held by SCW.		
Target audience:	All staff		
Committee/group consulted:	DDaT Strategy and Assurance Committee		
Monitoring arrangements and indicators:	This policy will be monitored by the DDaT Strategy and Assurance Committee to ensure any legislative changes that occur before the review date are incorporated.		
Training/resource implications:	Dissemination will take place using the Staff bulletin and will be displayed on the intranet corporate IT policies pages		
Approved and ratified by:	DDAT Senior Leadership Team Board	Date: 18/07/2023	
Equality Impact Assessment:	Yes	Date: 02/07/2023	

Date Issued:	18/07/2023	Review Date:	17/07/2023
Practice Owner	Technical Governance Lead		
Policy Owner	Cyber Security Manager		
Lead Director:	Simon Sturgeon – Chief Digital Information Officer		

Version control Change record

Date	Author	Version	Page	Reason for change
22/07/2021	Arif Gulzar	4.0	All	Version reset after ratification from SCW Corporate Governance and Assurance Group (CGAG)
05/06/2023	Arif Gulzar Richard Brady	4.1	All	Policy and Templates updates to include Sustainability, DSPT, NIS and addition of Clear Desk and Clear Screen.
04/07/2023	Arif Gulzar	4.2		Version for approval and ratification
18/07/2023	Arif Gulzar	5.0		Approved by DDaT Senior Leadership Team Board

Reviewers / contributors

Date	Name	Version	Position
05/06/2023	Arif Gulzar	4.1	Cyber Security Manager
05/06/2023	Richard Brady	4.1	Technical Governance Lead
20/06/2023	DDaT Strategy & Assurance Committee	4.1	Assurance Committee

Contents

1. Introduction and Purpose

Information and Cyber Security has critical importance to NHS patient care, information assets and other related business processes. High quality information underpins the delivery of high-quality evidence-based healthcare. Without effective security, NHS information assets may become unreliable, may not be accessible when needed, or may be compromised by unauthorised third parties. Information, whether in paper or electronic form, is of high importance to the NHS South, Central and West Commissioning Support Unit (SCW), therefore the organisation must ensure that the information is properly protected and is reliably available.

Information Security is primarily about people but is facilitated by the appropriate use of technology. The business benefits of this policy and associated guidance are:

- Assurance that all SCW information is being managed securely and consistently and in line with SCW associated policies and guidance.
- Assurance that SCW is providing a secure and trusted environment for the management of information used in delivering its business.
- Clarity over the personal responsibilities around information security expected of staff (as defined in the scope) when working on SCW business.
- A strengthened position in the event of any legal action that may be taken against the SCW (assuming the proper application of the policy and compliance with it).
- Demonstration of best practice in Information Security.
- Assurance that information is accessible only to those authorised to have access.

The requirements within this Policy are driven by the Data Protection Legislation covering security and confidentiality of personal information, including the UK General Data Protection Regulation and the Data Protection Act 2018.

ITIL 4 introduce the concept of Practices which are a set of resources designed to perform work and accomplish objectives. In addition to the resources, they align the capabilities of the organisation to complete the process and procedures. ITIL 4 groups practices into 3 areas:

- Management Practices
- Service Management Practices

- Technical Management Practices

This policy supports a number of Practices but is primarily aligned to the Information Security Management which is an ITIL Management Practice.

2. Scope and definitions

2.1. Scope

This policy applies to all SCW staff. Compliance and responsibility also extend to those contracted by the SCW as 3rd Party suppliers, contractors, NHS professionals, temporary staff, voluntary organisations and anyone duly authorised to view or work with SCW's information. All references to Information Security are inclusive of Cyber Security measures.

The purpose of this Information Security Policy is to protect, to a consistently high standard, all information assets, including patient and staff (as defined in the scope) records and other NHS corporate information, from all potentially damaging threats, whether internal or external, deliberate or accidental. SCW has a legal obligation to ensure that there is adequate provision for the security management of the information resources the organisation owns, controls, or uses. This Information Security Policy forms part of a suite of Information Governance documentation including but not limited to: Information Governance Policy, Confidentiality and Safe Haven Policy, and the Records Management Policy.

This Information Security Policy covers all forms of information held by the SCW, including

but not limited to:

- Information about members of the public and patients
- Non SCW staff on SCW premises
- Staff (as defined in the scope) and Personnel Information
- Organisational, Business and Operational Information

This Information Security Policy applies to all aspects of information handling, including, but not limited to:

Structured Record Systems – paper and electronic

Information Recording and Processing Systems – Paper, Electronic, Video, Photographic and Audio Recordings.

Information Transmission Systems, such as email, portable media, post and telephone.

2.2. Definitions

Asset - Anything that has value to the organisation, its business operations and its continuity.

Authentication - The organisation must ensure that the identity of a subject or resource is the one claimed.

Availability - The property of being accessible and usable upon demand by an authorised entity.

Business Impact = The result of an information security incident on business functions and the effect that a business interruption might have upon them.

Confidentiality - Everyone working in or for the NHS has the responsibility to use information and data in a secure and confidential way. Staff who have access to information about individuals (whether patients, staff or others) need to use it effectively, whilst maintaining appropriate levels of confidentiality. This policy sets out the key principles and main ‘do’s and don’ts’ that everyone should follow to achieve this for both electronic and paper records.

The common law duty of confidentiality requires that information that has been provided in confidence may be disclosed only for the purposes that the subject has been informed about and has consented to unless there is a statutory or court order requirement to do otherwise.

What is Personal Data - As described in part 1, subsection 3 of the Data Protection act 2018

(2) “Personal data” means any information relating to an identified or identifiable living individual

(3) “Identifiable living individual” means a living individual who can be identified, directly or indirectly, in particular by reference to—

(a) An identifier such as a name, an identification number, location data or an online identifier, or

(b) One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual

What are "Special Categories of Personal Data" - As described in article 9 of UK GDPR, special categories of personal data are Personal Data revealing:

a) racial or ethnic origin
b) political opinions
c) religious or philosophical beliefs
d) trade union membership
e) the processing of genetic data
f) biometric data for the purpose of uniquely identifying a natural person
g) data concerning health or
h) data concerning a natural person's sex life or sexual orientation

Under the **Data Protection legislation** staff can only process or have access to personal data if:

- An appropriate condition for processing (UK GDPR Article 6 and Article 9) and where necessary a supporting lawful basis has been identified and documented in a statutorily required Data Protection Impact Assessment (DPIA) or,
- Explicit consent has been obtained from the individual or,
- The data has been anonymised or pseudonymised in line with Data Protection legislation requirements; or
- The data is in respect of safety, safeguarding or in the public interest. Any decision taken to share Personal or Special Categories of Personal Data that is by its nature, owed a duty of confidentiality because of the above should be discussed with the SCW DPO/DDPO, documented in the DPIA and agreed by the Caldicott Guardian in liaison with the commissioning authority as appropriate.
- Staff should check with the SCW IG Lead if they have any queries on whether to access or process Personal or Special Categories of Personal Data.

Personal Confidential Data - Although an organisation within the NHS may have identified a lawful basis to process data, including special categories of personal data, this does not

necessarily mean that the information can be used or shared in a way that identifies the individual if that information has been obtained where a 'duty of confidence' is owed.

In practical terms this means that if a GP wanted to share information with another care organisation that is providing care to that Patient e.g., an acute or community hospital, as long as the GP believes that the Patient would raise no objection and that it would be within their reasonable expectations for them to do this then this sharing is permitted and encouraged within the law. However, if the GP wishes to share information that identifies a Patient and was obtained confidentially with someone else e.g. a charity, an advocate or a CCG, unless there are reasons why this must happen due to statutory obligations or it is in the public interest to do so, the Patient must be given the opportunity to consent to this happening.

It may be easier to consider the following table.

What information?	Category of data	How was it obtained?	Is it confidential data?
Name and address and postcode	Personal Data	Electoral register	No
Full Postcode, recent hospital admissions, age, marital status	Personal Data and Special category of personal data	Performance report	Yes – measures to reduce the risk of identifying the person should be taken by reducing the postcode search criteria
Member of local church	Special Category of Personal Data	Facebook members group post	No – made public by the individual
Religious belief limiting health care	Special Category of Personal Data	Patient to GP consultation	Yes – GP would only share if Patient would expect this for their care
Date of surgery on knee	Special Category of Personal Data	Individual posted photo of themselves in hospital	No – made public by the individual
Date of surgery on knee	Special Category of Personal Data	GP included in request for further funding for additional operation	Yes – GP would only share if Patient would expect this for their care
Sexual orientation	Special Category of Personal Data	Identifies own orientation on social media or	No – made public by the individual

		another public forum	
Sexual orientation	Special Category of Personal Data	Consultant includes information on gender reassignment status within hospital record	Yes – highly confidential and Consultant would only share if Patient would expect this for their care or has given explicit consent

Commercially confidential data - This describes information that is owed a duty of confidentiality concerning the organisation and its business. This includes trade secrets, parts of the procurement and contracting process and information it may hold that has been given to it by a third party. Further guidance on what constitutes commercially confidential data can be found here ICO guidance.

Cyber Security - Information and Cyber Security concerns the comprehensive risk management, protection and resilience of data processing and the digital networks that connect them.

Impact - The result of an information security incident, caused by threat, which affects assets.

Information Assurance - The confidence that information assets will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.

Information Security - The preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability and reliability can also be involved.

Staff - All SCW staff, those employed by SCW as contractors, NHS professionals, temporary staff, voluntary organisations and anyone duly authorised to view or work with SCW's information.

.

3. Details of the policy

This Information Security Policy will achieve a consistent approach to the security management of information throughout SCW and will aim to deliver continuous business

capability and minimise both the likelihood of occurrence and the impacts of information security incidents.

Security of our information is paramount, and the protective measures put in place, must ensure that Information Governance (IG) requirements are satisfied. The aim of this process is maintaining the confidentiality, integrity, and availability of SCW's information. To conform to the Information Security Assurance requirements of the Data Security and Protection Toolkit SCW shall:

Maintain the Confidentiality of Personal Information including patient and staff (as defined in the scope) identifiable information by protecting it in accordance with NHS Information Security Code of Practice, Data Protection Legislation, Caldicott Principles and other legal and regulatory framework criteria.

Ensure the integrity of SCW information by developing, monitoring and maintaining it to a satisfactory level of quality for use within the relevant areas.

Implement the necessary measures to maintain availability of SCW information systems and services. This includes putting in place contingency measures to ensure the minimum of disruption caused to SCW information systems and services.

This Information Security Policy is consistent with and supports SCW's policies and existing methods of working, which take precedence on any specific issue, and is in accordance with NHS national guidance.

3.1. Physical Security

The physical security of SCW information is the responsibility of all staff (as defined in the scope). The protection of both personal and confidential information is paramount in maintaining confidentiality, and users of SCW information must comply with the suite of Information Governance documentation. This is a local Information Security Policy to protect the information stored, processed and exchanged between SCW and other organisations.

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an appropriate confidentiality clause. Information security expectations of staff shall be included within appropriate job definitions.

Staff shall accept full responsibility for the security of information and information assets which are issued to them, taking necessary precautions to avoid loss, theft or damage. Information should not be left unattended in a public place or left in vehicles either on view, unattended or overnight. In the event of such an incident, Staff must report this immediately to the Information Governance team who will assist with the management of the incident.

During the COVID-19 pandemic many members of staff are working from home on a more permanent basis. Special care will need to be taken by staff to ensure the security of both information and hardware. This includes the security of a home office and equipment and the destruction of any sensitive printed material.

All access to personal and confidential information (whether on paper or electronically) located within SCW property must be controlled using the approved security measures. Advice and guidance can be sought from SCW IG Team or the IT hosted service. Access to information shall be restricted to users who have an authorised business need and access has been approved by the relevant Information Asset Owner (IAO). Other staff responsibilities include ensuring perimeter security by making sure that security doors are closed properly, blinds drawn, and that any door entry codes are changed regularly.

All staff must wear identification badges and individuals not wearing identification in areas which are not for public access should be challenged. Visitors should be met at reception points and always accompanied even when leaving the building. Identification badges should be surrendered on termination of contract along with door keys, Smartcards and all other equipment provided by or belonging to SCW.

Portable devices that are intended for use with personal or confidential information must be supplied and supported by SCW. Where it is not practical for contractors or interim staff to obtain approved devices personal or confidential information must not be transferred and a suitable device should be sought.

Each team is responsible for holding an information asset register which details the specification, user and location of the asset. IT equipment will be security marked and its serial number should be recorded. It is the responsibility of the area's assigned Information Asset Administrator to update the asset register and submit to the SCW IG Team.

Each team will have a designated Information Asset Owner (IAO) who is responsible for all information held and used by that team.

Management of computers and networks shall be controlled through standard documented procedures. Agreed contracts with third party suppliers working for and on behalf of SCW must adhere to SCW policies and procedures.

3.2. Protection from Malicious Software

All IT equipment used by SCW staff (as defined in the scope) is protected by countermeasures and management procedures to protect against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation's property without approval from the SCW IT Service Desk/ Service Portfolio Manager. Users breaching this requirement may be subject to disciplinary action.

3.3. Preventing Information Security Breaches

Each SCW Team is responsible for regularly monitoring the information they hold and use. An annual mapping exercise of information flows in and out of the teams will be undertaken. This exercise will allow any information risks to be identified by each team and appropriate action to mitigate those risks should be taken. It is the responsibility of the IAO to ensure that this takes place.

Protection against unauthorised access or disclosure:

Staff (as defined in the scope) have the responsibility to ensure that information is always kept secure by adhering to the following:

- Screens should be locked when unattended even for short periods of time,
- Registration Authority Policy (and procedures)
- Password policy
- Internet and email policies,
- Remote Working and Portable Devices Policy
- Guidance provided on the use of phones and post which can be found within the Safe Haven Policy.

- Disposal of equipment

For the secure transfer of bulk electronic information, secure file transfer function within NHSmail should be used as it has the approved levels of encryption.

SCW will ensure that paper information is secure by following adequate records management procedures and processes. Staff should have access to secure storage areas and if possible, a clear desk routine should be followed. Should a legitimate need arise for local storage or a non-routine transfer of personal or confidential information then a risk assessment must be undertaken first, and the justification approved by the SIRO and recorded by the line manager. SCW staff must also ensure when moving away from desks that they do not leave personal or confidential information accessible.

SCW promotes a 'paper lite' environment through use of electronic devices to transform information to a secure electronic form.

Any non-routine bulk extracts (50+ records) or transfers of information must be authorised by the responsible Director or the Information Asset Owner for the work area and may require approval by the Senior Information Risk Owner.

That the integrity and value of the information is maintained: The organisation ensures that staff and contracted individuals are aware and apply the Data Protection Legislation and Caldicott Principles through their working practices. The SCW Information Governance Team promotes the principles and provides or facilitates training.

That information shall be available to properly authorised personnel as and when it is required: All staff is required to use the guidance contained in the NHS Confidentiality Code of Practice, Care Record Guarantee and the Records Management Code of Practice. The Information Governance suite of policies provides further guidance.

Organisation-wide business continuity plans for information systems are in place: This includes identification and assessment of critical dependencies on SCW information resources. The organisation will implement a business continuity management system (BCMS) that will be aligned to the international standard of best practice (ISO 22301 –

Societal Security – Business Continuity Management Systems). Business Impact Analysis will be undertaken in all areas of the organisation.

Business continuity plans will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident. The SIRO has a responsibility to ensure that appropriate disaster recovery plans are in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis.

Relevant Information Security Training and awareness is available to staff via the NHS Digital provided Information Governance Training Modules. Additional training needs beyond this will be assessed.

All breaches of information security, actual, suspected, or near misses are recorded on Datix, and reported using IG and Cyber Incident Management and Reporting Procedure.

3.4. Potential or Actual Security Breaches

All staff (as defined in the scope) are responsible for ensuring that no potential or actual security breaches occur because of their actions. SCW IG Team will investigate all suspected / actual security breaches.

The SCW IG Team and the Risk Management lead must be informed of all security issues using Datix to ensure that the appropriate investigations are carried out. The SCW Registration Authority (RA) Manager will also receive copies of any Registration Authority related security breaches or incidents.

The resulting Root Cause Analysis (RCA) report will specify, details of suspected incident, assets affected or compromised, and investigation conducted. Recovery/contingency plans, damage and risk classification and recommendations will be provided.

All incidents will be investigated immediately and reported as part of SCW IG and Cyber Incident Management and Reporting Procedure and in the case of serious incidents to the NHS England Data Protection officer after review by the SCW Deputy Data Protection Officer. Reports and recommendations will be approved and monitored by IT senior leadership team and the Information Governance Steering Group.

3.5. Risk

SCW will need to ensure that adequate audit provision is in place to ensure continuing effectiveness of information security management arrangements.

Any security measures must be viewed as necessary protection against a risk of an event occurring or to reduce the impact of such an event. Some of these events may be deliberate acts of damage and others may be accidental. Nevertheless, a range of security measures can be deployed to address:

- The ***Threat*** of something damaging the confidentiality, integrity or availability of information held on systems or manual records.
- The ***Impact*** that such a threat would have if it occurred.
- The Likelihood of such a threat occurring.

All staff (as defined in the scope) should consider the risks associated with the computers they use and the information that is held on them, as well as information held in manual records.

All staff are responsible for reporting any apparent shortcomings of security measures currently employed to address these risks to the Head of Governance Services within SCW.

3.6. Information Disposal

Electronic (See Informatics disposal policy for more detail)

Computer assets must be disposed of in accordance with SCW disposal of confidential waste procedure. This includes removable computer media, such as hard drives, external storage drives, USB drives, Memory cards, tapes and disks.

All data storage devices must be purged of personal and confidential data before disposal. Where this is not possible, the equipment or media must be destroyed by a technical waste service provider. For further information, please contact SCW's asset management team.

Paper - Sensitive printed material should be confidentially destroyed using an appropriate method such as shredding. Where SCW has large quantities of confidential waste which need to be disposed of, the IG team can help facilitate this through an approved secure shredding contractor.

3.7. Security of third-party access to NHS Networks

Written agreement must be received from all external contractors and non-NHS parties that they agree to treat all information confidentially and that information will not be disclosed to unauthorised individuals. Such contractors should also sign a declaration that they understand the relevant legislation should they need to access personal or confidential information stored on a computer system. This declaration is available from SCW Information Governance team.

3.8. New or Existing Programmes and Projects

Under UK General Data Protection Regulations, the completion of a Data Protection Impact Assessment (DPIA) is a statutory requirement where the processing of health / medical personal data is being considered. The Information Governance Team will review, and risk assess the proposed processing through the DPIA process. All resulting escalations are referred to the SCW Information Governance Steering Group as a subgroup of Corporate Governance and Assurance group. Please refer to the Data Protection Impact Assessment Framework and supporting guidance for further information on this statutory requirement. Under section 157 of the Data Protection Act 2018, the ICO can impose a penalty for failing to complete a DPIA when it is mandated to do so under Article 35 of UK GDPR. The maximum amount that can be imposed is £17.5 million or 4% of total annual worldwide turnover in the case of an undertaking or group of undertakings.

3.9. Clear Desk

When leaving a desk for a short period of time, users must ensure printed matter containing information that is considered confidential is not left in view.

When leaving a desk for a longer period / overnight, users must ensure printed matter containing confidential information is securely locked away. Whiteboards and flipcharts should be wiped / removed of all confidential information when finished with.

3.10. Clear Screen

When leaving the workstation for any period of time, the user must ensure they lock their computer session to prevent un-authorised access to the network and stored information.

All users must ensure their screens cannot be overlooked by members of the public, or people without the necessary authority when confidential data and/or information is displayed. Where appropriate, privacy filters should be used protect the information.

During the COVID-19 pandemic many members of staff are working from home on a more permanent basis. Special care will need to be taken by staff to ensure the security of both information and hardware. This includes the security of a home office and equipment and the destruction of any sensitive printed material.

All users are responsible for the information that is displayed on the screens whilst computer/laptop is being supported remotely by IT service desk or when in a webinar/Teams call.

Following up to a maximum 10 to 15 minutes of inactivity (depending on user group), the session will be automatically locked as a failsafe measure.

4. Roles and Responsibilities

SCW Managing Director - SCW Managing Director has overall responsibility for Information Governance within the organisation. As Accountable Officer, they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. The management of information risk and information governance practice is now required within the Statement of Internal Control which the Accountable Officer is required to sign annually.

SCW Senior Information Risk Owner (SIRO) - The Senior Information Risk Owner for SCW is an executive management team member with allocated lead responsibility for the organisation's information risks and provides the focus for management of information risk at executive management level. The SIRO must provide the Accountable Officer with assurance that information risk is being managed appropriately and effectively across the organisation and for any services contracted by the organisation. The SCW Information Governance Team will support the SIRO in fulfilling this role.

SCW Caldicott Guardian - The Caldicott Guardian is the person within SCW with overall responsibility for protecting the confidentiality of information that includes personal data and special categories of personal data, and for ensuring it is shared appropriately and in a secure

manner. This role has the responsibility to advise the SCW Executive Management Team on confidentiality issues. SCW Information Governance Team will support the Caldicott Guardian in fulfilling this role.

SCW Deputy Data Protection Officer -The Deputy Data Protection Officer (DDPO) is the person within SCW that has been identified to support the role of the Data Protection Officer (DPO) in NHS England. This role has the responsibilities as set out in UK GDPR guidance as delegated duties from the DPO and is responsible to feedback any Information Governance issues to SCW Executive Management Team and the DPO at NHS England. The DDPO will ensure that where an incident is likely to result in a risk to the rights and freedoms of Data Subjects the ICO (Information Commissioner's Office) is informed no later than 72 hours after the organisation becomes aware of the incident. They will also be part of the Data Protection Impact Assessment (DPIA) process on behalf of SCW.

SCW Information Governance Team - SCW Information Governance Team is responsible for ensuring that the Information Governance programme is implemented throughout the organisation. The team is also responsible for the completion and annual submission of the Data Security and Protection Toolkit for SCW. The Information Governance Team will support the organisation in investigating IG and Cyber Serious Incidents Requiring Investigation (SIRI), offer advice and ensure the organisation complies with legislation, policies and protocols.

SCW Information Asset Owners (IAO) - The SIRO is supported by Information Asset Owners (IAOs). The role of the IAO is to understand what data and information is held, what is added and what is removed, who has access and why in their own area. As a result, they are able to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of the assets. The Information Governance Team will support the IAOs in fulfilling their role.

SCW Information Asset Administrators (IAAs) - Information Asset Administrator are required to support the IAO's and SCW SIRO who will work with the Information Governance Team to ensure staff apply the Data Protection Legislation and Caldicott Principles within working practices. The Information Governance Team will provide local face to face IG

training if required and will monitor staff compliance by way of the ESR portal and link to the e-LfH platform.

Cyber Security Manager - Acting as a central point of contact on IT security within the organisation and for external organisations that has entered into an agreement for the provision of IT services by SCW. Implementing an effective framework for the management of security. Assisting in the formulation of Information Security Policy and related policies.

Advise on the content and implementation of the Information Security Programme.

Co-ordinate IT security activities particularly those related to shared information systems or IT infrastructures.

Liaise with external organisations on IT security matters, including representing the organisation on cross-community committees.

Advising users of information systems, applications and Networks of their responsibilities.

Creating, maintaining, giving guidance on and overseeing the implementation of IT Security.

Ensuring that risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk.

Ensure breaches of policy and recommended actions are reported in line with organisation's procedures.

All Staff - All staff working for, on behalf of, or whose organisation that has entered into an agreement for the provision of IT services by SCW have a general responsibility for the security of information they create or use in the course of their duties. They should ensure they are aware of all the relevant information security policies and procedures and follow their recognised codes of conduct. NHS staff have a legal duty of confidentiality to keep information about individuals confidential.

All staff must abide by this and associated policies and procedures.

All staff should report any suspected breaches of this policy to their line manager or the assigned Information Asset Administrator and the SCW IG team.

All staff must be aware and understand that failure to comply with the rules regulations contained within this policy, may result in disciplinary action.

5. Training

SCW requires that staff recognise the importance of appropriate information handling which incorporates statutory, common law and best practice requirements. As Information Governance is a framework drawing these requirements together, it is important that staff receive the appropriate training.

The NHS Operating Framework 'Informatics Planning' requires that the organisation ensures all staff receive annual basic Information Governance training appropriate to their role through the online NHS Information Governance Training Tool or from their IG manager. Managers are responsible for monitoring staff) compliance.

SCW staff will receive an Information Governance staff Handbook on joining the organisation. Staff will be required to sign and return a receipt to the SCW IG Team to evidence their compliance.

6. Public sector equality duty - Equality Impact Assessment

The Equality Act 2010 requires public bodies to consider the needs of all individuals in their day-to-day work. At SCW we do this by completing an Equality Impact Assessment as described in the Equality and Diversity Policy which for this policy can be found in Appendix A.

7. Sustainability Impact Assessment

This policy will be delivered in alignment with the SCW Sustainability strategic aim.

ITIL defines sustainability as "A business approach focused on creating long-term value for society and other stakeholders, by addressing the risks and opportunities associated with economic, environmental and social developments."

This policy supports the strategy in a number of ways including but not limited to:

- Ensure regulatory compliance to safeguard the business from breaches and potential fines.

- Reduce the risk of cyber-attacks and incidents.
- Help to prevent the environmental impact that could result from cyber-attacks.
- Security and sustainability as interconnected priorities, it can help to ensure that SCW operations are both secure and environmentally friendly.
- Improve energy efficiency as security vulnerable software and hardware can consume more energy than newer, more efficient alternatives. By implementing Information Security Policy can help to reduce energy consumption and minimise its carbon footprint.
- Standardise rules and processes that protect against vectors threatening data integrity, availability, and confidentiality.

8. Success Criteria/Monitoring of the Effectiveness of the Policy

SCW Informatics Senior Leadership Team and Information Governance Steering group are responsible for the approval of this policy. SCW Corporate Governance Assurance Group will then ratify that approval.

SCW's Senior Information Risk Owner (SIRO), Information Asset Owners and Data Custodians are responsible for the implementation of this policy throughout the organisation.

Regular audits should be undertaken to ensure that all portable computing and mobile devices issued can be accounted for and that assurance is provided to the Senior Information Risk Owner (SIRO) that identified risks are adequately controlled and managed. These will be presented to the DDaT Strategy and Assurance Group as part of the Quarterly Cyber Report for SCW.

Adherence to this policy will be monitored via investigation and analysis of information security incidents reported via the approved incident management process.

9. Review

The SCW Informatics Senior leadership team and Information Governance Steering Group are responsible for the review of this policy. This policy will be reviewed after 2 years of it's issue or following major legislative or organisational change.

10. References and associated documents

- Information Governance Policy and Framework
- Confidentiality and Safe Haven Policy
- Information Security Management: NHS Code of Practice
- NHS Records Management: Code of Practice
- SCW Records Management Policy
- NHS England Information Security Policy
- SCW Information Governance Policy
- SCW Data Protection Impact Assessment framework
- SCW Information Governance Staff Handbook
- Asset Management Policy
- Review of Data Security Consent and Opt-Outs
- Remote Working and Portable Devices Policy
- SCW DDaT Incident Management Policy
- SCW Risk Management Policy
- SCW IG and Cyber Incident Management & Reporting Procedure
- SCW Information Security Management Process
- Network and Information System Regulations (NIS Regulations) 2018

11. Confidentiality Agreement

Data Sharing and/or Data Processing Agreements may be issued for signature by third-party organisations where appropriate, following completion of a Data Protection Impact Assessment. A confidentiality agreement may also be a requirement, which shall be dependent upon the purpose of the data sharing or processing involved. For the latest Confidentiality Agreement templates, please contact Information Governance team.

Appendix A - Equality Impact Assessment

1 What is it about? *Refer to the Equality Act 2010*	
Information Security Policy	
a) Describe the proposal/policy and the outcomes/benefits you are hoping to achieve	
The objective of this Information Security Policy is to safeguard the confidentiality, integrity and availability of information, information systems, applications and networks owned or held by SCW.	
b) Who is it for?	
All Staff	
c) How will the proposal/policy meet the equality duties?	
The policy will have no adverse effect on equality duties.	
d) What are the barriers to meeting this potential?	
There are no barriers currently identified.	
2 Who is using it? *Consider all equality groups*	
a) Describe the current/proposed beneficiaries and include an equality profile if possible	
The policy is applicable to all staff.	
b) How have you/can you involve your patients/service users in developing the proposal/policy?	
Patients and service users have not been involved in developing this policy as this is an operational IT Policy in response to legislative requirements.	
c) Who is missing? Do you need to fill any gaps in your data?	
There are no gaps.	
3 Impact *Consider how it affects different dimensions of equality and equality groups*	
Using the information from steps 1 & 2 above:	
a) Does (or could) the proposal/policy create an adverse impact for some groups or individuals? Is it clear what this is?	
It is not anticipated that any adverse impact will be created.	
b) What can be done to change this impact? If it can't be changed, how can this impact be mitigated or justified?	
Not applicable	

c) Does (or could) the proposal/policy create a benefit for a particular group? Is it clear what this is? Can you maximise the benefits for other disadvantaged groups? This policy is equal across all groups.
d) Is further consultation needed? How will the assumptions made in this analysis be tested? No
4 So what (outcome of this EIA)? ***Link to the business planning process***
a) What changes have you made in the course of this EIA? None
b) What will you do now and what will be included in future planning? Nothing
c) When will this EIA be reviewed? At next policy review.
d) How will success be measured? No equality issues are created.

Sign-off

Name of person leading this EIA: **Arif Gulzar – Cyber Security Manager**	Date completed: **02-07-2023** Proposed EIA review date: **02-07-2025**
Signature of director/decision-maker Name of director/decision-maker **Simon Sturgeon** **Chief Information Digital Officer**	Date signed