South, Central and West
Commissioning Support Unit

OFFICIAL

Network Security Policy

Version 5.0 July 2023

Document control

Document name	Version	Status	Author
Network Security Policy	5.0	Final	Paul Lambert - Senior Technical Consultant (Networks)
Document objectives:	The objective of this Policy is to safeguard the confidentiality, integrity and availability of information, information systems, applications hosted or managed within SCW networks from internal or external threats.		
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:	All Staff - 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: 08/06/2023	

Date Issued:	18/07/2023	Review Date:	17/07/2025
Practice Owner:	Head of Technical Operations		
Policy Owner:	Senior Technical Consultant (Networks)		
Lead Director:	Simon Sturgeon – Chief Digital Information Officer		

Version Control

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)
24/05/2023	Richard Brady	4.1	All	Template and branding updates
04/07/2023	Paul Lambert Richard Brady Arif Gulzar	4.2	All	Policy updates with reference to NIS, DSPT and Sustainability.
13/07/2023	Paul Lambert	4.3		For approval by SLT
18/07/2023	Paul Lambert	5.0		Approved by DDaT Senior Leadership Team Board

Reviewers / contributors

Date	Name	Version	Position
04/07/2023	Paul Lambert	4.2	Senior Technical Consultant (Networks)
04/07/2023	Richard Brady	4.2	Technical Governance Lead
04/07/2023	Arif Gulzar	4.2	Cyber Security Manager
13/07/2023	Strategy and Assurance Committee	4.2	Assurance and SME review

Contents

1 Introduction

This document defines the Network Security Policy for SCW. The Policy applies to all staff working directly for the SCW, and any organisation that has entered into an agreement for the provision of Informatics service by the SCW.

The policy applies to all business functions and information contained on the Network, the physical environment and relevant people who support the Network. The Network is a collection of communication equipment such as servers, computers, printers, and modems. The Network is created to share data, software, and peripherals such as printers, Internet connections, CD-ROM and tape drives, hard disks and other data storage equipment.

The Information Security Management System (ISMS)

The objective of the ISMS is to define a coherent set of policies, standards and architectures that: -

- Set out the governance of IT security
- Provide high level policy statements on the requirements for managing IT security
- Define the roles and responsibilities for implementing the Information security policy
- Identify key standards, processes and procedures to support the policy
- Define security architectures that encapsulate the policy and support the delivery of secure Informatics service

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

SCW is committed to developing effective policies, procedures and other corporate documents that deliver compliance with our necessary governance requirements including expectations of our host body, our customers and external assessment organisations. While SCW is hosted by the NHS Commissioning Board (NHS England), we will not develop or encourage arrangements that conflict with existing NHS England policies.

This policy applies to all Networks used for:

- The storage, sharing and transmission of non-clinical data and images

- The storage, sharing and transmission of clinical data and images on behalf of the SCW customers, for example, Continuing Health Care (CHC)
- Printing or scanning non-clinical or clinical data or images
- The provision of Internet systems for receiving, sending and storing non-clinical or clinical data or images

The aim of this policy is to ensure the security of the SCW Network and to do this, the organisation will:

- Ensure the protection of Network from unauthorised disclosure and accidental modification
- Ensure the accuracy and completeness of the organisation's IT assets

2.2 Definitions

ACL	Access Control List
Common Criteria (CC)	CC is a widely recognised international scheme used to assure security-enforcing products. It provides formal recognition that a developer's claims about the security features of their product are valid and have been independently tested against recognised criteria, to a formalised methodology.
IAA	Information Asset Administrator
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarised Zone
DNS	Domain Name System
DSPT	Data Security and Protection Toolkit
EAL4	Common Criteria Evaluation Assurance Level 4
HSCN	Health and Social Care Network
HTTPS	Hypertext Transfer Protocol Secure
IAO	Information Asset Owner
ISO	International Standard Organisation
LAN	Local Area network
MPLS	Multi-Protocol Label Switching

SFTP	Secure File Transfer Protocol
SIRI	Serious Incidents Require Investigation
SIRO	Senior Information Risk Owner
SSH	Secure Shell
SSID	Service Set Identifier
VPN	Virtual Private Network

3 Details of the policy

3.1 Network Design

3.1.1 SCW operates with a 'defence in depth' approach to protecting IT systems. Central to this approach is multi-layered security to provide extensive protection to the network by ensuring that there is no single point of compromise to the network.

3.1.2 Wherever appropriate, SCW network shall be segmented into different zones based on customer, the sensitivity of information being contained and the level of exposure it has to the public/Internet. These zones must be segregated by implementing the most appropriate controls which include but are not limited to:

- Implementing internal and external firewalls
- Implementing DMZ firewalls
- Using MPLS, VPN and encryption to ensure the protection of data passing over networks

3.1.3 Shared networks shall have routing controls to ensure that computer connections and information flows do not breach access control policies.

3.1.4 The SCW network should be designed to avoid single points of failure and to provide high availability.

3.1.5 There must be a separation between development, test and operational environments to reduce the risk of unauthorised access or changes that will have an impact on the confidentiality, integrity and availability of the service.

3.1.6 Network diagrams (both logical and physical) that define the network topology, 'boundaries', IP addresses, core network hardware and software and configurations for all SCW networks must be maintained. This documentation must be sufficient to rebuild any network equipment in the event of its failure and replacement.

3.1.7 The Network must be approved by the Enterprise Architect and the Technical Operations team before it commences operation, ensuring the network does not pose an unacceptable security risk to the organisation and meets Data Security Protection Toolkit (DSPT) requirements and other Health and Social Care Network (HSCN) standards.

3.1.8 Wired connections and connection points

- Physical ports on firewalls and routers should be protected to prevent the creation of unauthorised access.
- All network equipment must be clearly labelled and documented to facilitate tracing from LAN to network equipment port.

3.1.9 Wireless connection and wireless access points

- Wireless connections must be implemented with approved protocols and strong security standards, including but not limited to enterprise-level encryption, authentication and certificates.
- Corporate wireless LAN must be segregated from the internet guest wireless LAN. Technical controls must be implemented to ensure this separation, including the use of different SSIDs.

3.2 Physical and Environmental Security

3.2.1 All network assets and components must be recorded in an asset inventory and assigned an owner, in accordance with the SCW Informatics Asset Management Policy.

3.2.2 Core networking equipment will be housed in controlled and secure environments and correctly maintained to enable its continued availability and integrity.

3.2.3 Critical or sensitive network equipment will be protected by a secure perimeter, with appropriate security and entry controls (including intruder alarms), fire suppression systems and in an environment that is monitored for temperature, humidity and power supply quality where appropriate.

3.2.4 Entry to secure areas with critical or sensitive network equipment will be restricted to those whose job requires it. The Technical Operations team will maintain and periodically review a list of those with unsupervised access to core SCW network/computer rooms.

3.2.5 The Technical Operations team are responsible for ensuring that access codes for core SCW computer/network rooms are changed periodically, following a known or suspected compromise of the code.

3.2.6 Smoking, eating and drinking is forbidden in areas that house critical or sensitive network equipment.

3.2.7 All visitor requests to secure network areas must be authorised by the Head of Service Delivery or the Technical Operations Manager.

3.2.8 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.

3.2.9 All visitors to secure network areas must be escorted by a Technical Operations team member and made aware of procedures for visitors.

3.3 Network Access Control

3.3.1 All access to the network mut be via a secure login procedure, designed to minimise the opportunity for unauthorised access.

3.3.2 Authentication is essential before any access is granted to the network. Appropriate authentication mechanisms must be implemented for users and devices connecting to the SCW network.

3.3.3 Access rights are 'Role Based', allocated on the requirements of the user's role rather than on a status basis.

3.4 Security Standards and Security Configurations

3.4.1 Networks shall be adequately maintained and controlled, to be protected from threats and to maintain security for the systems and applications using the network, including information in transit.

3.4.2 All SCW IT assets shall be assessed to determine exactly what business functionality is required; all unnecessary functionalities must be removed, and the default configurations updated. The assessment shall include Operating System Configuration, Applications, System Utilities, Network services & protocols and User/Logon accounts. This is the principle of 'secure by design'.

3.4.3 Baseline security configurations considering the secure by design requirements must be developed to ensure a consistent build status for all client and server systems and network equipment where possible. These configurations will be assessed annually as part of cyber essentials Plus assessment.

3.4.4 All managed IT network equipment must be security hardened using best practice standards to an appropriate level. This security hardening must be continually enforced using the appropriate technical controls.

3.4.5 TechOps networks team ensures to implement a baseline configuration procedure whereby network components have their administrative passwords changed from the

vendor supplied default passwords to help prevent a threat actor from being able to gain administrative access to the network devices.

3.4.6 Strong cryptographic encryption and secure authentication methods or protocols must be used for remote access and to transfer sensitive information and data such as SSH, HTTPS, SFTP. If not feasible then a risk assessment is to be conducted as part of SCW Change Control process.

3.4.7 Access to management ports or other administrator facilities must be securely controlled to ensure they are only available to the approved individuals within Technical Operations team.

3.4.8 The remote access or remote management interface to services must be configured to permit connection only from a limited range of administration IP addresses, thus ensuring that it is only available to the system administrators.

3.5 Firewall configuration & management

3.5.1 SCW is committed to operating fully resilient, enterprise-grade firewalls. All network perimeter firewalls must be accredited to common criteria EAL4 standard as a minimum.

3.5.2 Access to read or write firewall configurations for both internal and perimeter devices are to be strictly restricted and logged.

3.5.3 There must be an explicit DENY rule configured on all managed firewalls/routers for DSPT and Cyber Essentials Plus compliance.

3.5.4 All connections to the inside of external connection firewalls must terminate on a switch port or on a LAN that is dedicated to that connection.

3.5.5 Any requests to create, modify or delete an access control list (ACL) rule on a firewall must be approved as part of SCW Change Control process prior to implementation.

3.5.6 SCW Technical Operations team reserves the right to deny requests for changes to firewall configurations as per SCW change control process if the risk associated is deemed objectionable. An explanation of the associated risk will be provided to the requester and alternative solutions will be explored.

3.5.7 Firewall ACL rules and objects must be audited at least quarterly by the Technical Operations team to minimise the presence of legacy and potentially insecure rules that are no longer needed. The rules which are no longer required must be disabled/removed from the firewall or router configuration.

3.6 Connecting Equipment to the Network

3.6.1 Equipment must not be connected to the SCW network without the approval from the IT Service Desk.

3.6.2 A work request should be logged for new equipment or services to be hosted on the network and the appropriate change control must be logged to perform the risk assessments prior to such connection.

3.6.3 All equipment connected to the SCW network must be registered with SCW Informatics Asset Management team before it is connected.

3.6.4 As part of this registration, all equipment connected to the SCW network must be assigned an asset tag and unique name following the SCW naming convention to facilitate the easy identification of the location, ownership and purpose of the equipment.

3.6.5 Network address allocation within the SCW network is the responsibility of the Technical Operations team. The default configuration for allocating addresses to equipment will be via dynamic addressing (e.g., DHCP). Where equipment requires a fixed address, that address will be assigned by the Technical Operations team.

3.6.6 Dynamic address servers (e.g., DHCP servers) must be implemented only by Technical Operations. Address allocations will be maintained in central name services (e.g., DNS), and these will be used to resolve addresses.

3.6.7 Internal DNS servers will hold the internal information about this domain within the Active Directory or equivalent.

3.6.8 Internal DNS servers will also provide a means for the resolution of external fully qualified domain names.

3.7 Third party and external network connections

3.7.1 Third party or external access to the network poses significant risk and therefore must be appropriately managed.

3.7.2 Third party access to the SCW network will be based on a formal contract that satisfies all necessary NHS security requirements and network agreements.

3.7.3 All third-party connection requests to the SCW network must reviewed and approved by Change Advisory Board (CAB). This includes formal agreements for the exchange of data between SCW and external organisations.

3.7.4 As part of change control, a risk assessment shall be conducted to identify risks associated with access to information and information processing facilities by the third party, and the appropriate controls implemented.

3.7.5 Unsolicited network traffic (excluding email traffic or approved third party support access) that originates from outside SCW network boundaries should not be permitted to directly enter the internal network. Appropriate technical measures should be implemented to ensure adequate separation of internal and external traffic.

3.7.6 Connections between the SCW network and public networks (e.g., the Internet) must be protected by firewalls.

3.7.7 Currently no third party (other than those approved) has any access rights to SCW managed networks and systems.

3.8 Configuration Backup and Restoration

3.8.1 The Technical Operations Manager is responsible for ensuring that configuration of networking equipment i.e., firewalls, routers and switches is backed up regularly in accordance with the Informatics Backup policy.

3.8.2 Documented procedures for the backup and restoration process must be produced and communicated to all relevant staff in the Technical Operations team.

3.8.3 The disposal of networking equipment must comply with Informatics IT Disposal policy.

3.9 Risk Assessment

3.9.1 SCW will ensure that risk assessments are conducted on managed network. These assessments will test and identify the appropriate security countermeasures necessary to protect the network from breaches in Confidentiality, Integrity and Availability and determine the compliance with industry standards such as Cyber Essentials Plus and DSPT.

3.9.2 Vulnerability risk assessments will be conducted on the network annually as part of the Cyber Essential Plus Accreditation; the scope of this assessment will depend on the area of the network that needs to be assessed. In addition to this assessment, monthly network perimeter vulnerability assessments will be performed, and remedial actions will be taken to mitigate high severity security risks.

3.10 Network Monitoring

3.10.1 All network IP addresses in use on the SCW network must be recorded by the Technical Operations team.

3.10.2 All managed network equipment must be monitored using a network monitoring system.

3.10.3 Network equipment must be configured to record an audit trail for unauthorised access and the audit trail must be protected from tampering. These logs must be retained for at least 3 months in a log management system.

3.10.4 SCW Technical Operations team must carry out routine performance monitoring of the SCW network and propose corrective action where traffic levels cause bottlenecks. Performance monitoring will include at least availability, collision rates and error rates.

3.10.5 Traffic monitoring is permitted by Technical Operations team in support of troubleshooting and planning activity, but data must be deleted once it is no longer required for this purpose. Packet capture is strictly permitted for Technical Operations team only, for the purpose of investigating any real or suspected security incident.

3.10.6 When capturing traffic for troubleshooting and monitoring purposes, the network administrator must ensure this does not lead to the inappropriate disclosure of sensitive information.

3.10.7 All incidents identified on the network are to be reported and tracked in accordance with SCW Incident Management process, including security incidents.

3.10.8 For all managed systems, the SCW Technical Operations team will ensure that detective, protective and corrective measures are in place to safeguard the network from viruses and other malicious software.

4 Incident – Reporting, Investigations and Resolutions

All staff should ensure that they report actual/potential security incidents as soon as they become aware to IT Service Desk and Information Asset Administrator.

All incidents, investigations and resolutions will be recorded on the Service Desk system for reporting, knowledge base and future learning.

There may be instances where incidents are reported directly to the Cyber Security team or Information Governance due to their sensitivity using SCW incident management system (DATIX). These are likely to be legal and/or forensic incidents which will be dealt with according to the SCW IG/Cyber Incident Management and Reporting Procedure.

Incident reporting, investigation and resolutions within the policy are completed with reference to and in line with the SCW Information Governance and Cyber Incident Management and Reporting Procedure. This sets out how SCW will ensure robust breach detection and internal reporting procedures are in place that comply with legislative timescales and is aligned to The Security of Network and Information Systems Regulations 2018 (“NIS Regulations”). The NIS regulations seek to ensure that essential services, including healthcare, have adequate data and cyber security measures in place to deal with the increasing volume of cyber threats. They require ‘operators of essential services’ to report any

network and information systems incident which has a ‘significant impact’ on the continuity of the essential service that they provide to the relevant ‘competent authority’. For further information see Information Governance and Cyber Incident Management and Reporting Procedure Version 4.6 (Internal SCW link).

5 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 the 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 Serious Incidents Requiring Investigation (SIRIs), 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 Administrators 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 consult OD portal and link to the e-LfH platform.

Cyber Security Manager

Responsibilities of the Cyber Security Manager include:

- 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 informatics service by the 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 Informatics service by the 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.

6 Monitoring and Audit

To provide assurances that controls in place are working effectively, the Cyber Security Manager will work closely with the SCW IG team to ensure that audits of systems and access controls to networks are conducted on a regular basis at least annually. Examples of events that will be audited will include frequency, circumstances and location.

- Failed attempts to access confidential information
- Repeated attempt to access confidential information
- Shared login and passwords

SCW will ensure that:

- There is continuous improvement in complying with the common law duty of confidentiality and data protection legislation and learning outcomes.
- Ad-hoc network availability and uptime reports are produced using network monitoring tools when requested by customers
- All incidents are audited to ensure any recommendations made have been implemented
- An action plan and action outcome are developed in the event of a breach to the SCW Networks
- Learning outcomes will be shared with other directorates/departments to prevent similar incidents from reoccurring.

This will ensure that the SCW fully embeds improvements to its information governance structure and demonstrate it is proactive in assessing and preventing information risk.

Reporting requirements will be reviewed annually to ensure they are aligned to assurance controls requested by but not limited to Cyber Essentials Plus, Service Desk Institute, NIS Regulations, Data Security & Protection Toolkit, Internal and external audit.

7 Dissemination and Implementation

This document will be published on the SCW intranet. Information Asset Owners and other senior managers are required to ensure that their staff understands its application to their practice.

Organisations that have entered into an agreement for the provision of Informatics service by the SCW should ensure that this document and other IT related documents are cascaded to their staff.

Awareness of any new content or change in process will be through electronic channels e.g., through email, in staff bulletins etc. Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the SCW IG team.

8 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 which, for this policy, can be found in Appendix A.

9 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.
- System monitoring takes place in line with this policy which enable the proactive resolution of service impacting incidents with maintains SCW reputation as a service provider.
- Hardware and software is maintained at a vendor supported version level to ensure resolution of incidents in line with target KPIs maintaining SCW reputation as a service provider.
- The life-cycle management of new hardware is completed in line with sustainability guidance and at an as low as possible environmental footprint.

10 Review

In line with the SCW’s key documents, this document will be reviewed no later than 2 years from the date of original circulation unless new, revised legislation or national guidance necessitates an earlier review.

11 References and associated documents

The following documentation relates to the management of information and together underpins the SCW's Information Governance Assurance Framework. This procedure should be read in conjunction other policies:

- Information Governance Framework Policy
- Information Security Policy
- Access Control Policy
- Password Policy
- Business Continuity Plans
- SCW Information Governance and Cyber Incident Management and Reporting Procedure
- DDaT Incident Management Process
- The HSCN Connection Agreement

Appendix A - Equality Impact Assessment

1 What is it about? ***Refer to the Equality Act 2010*** Network Security Policy
a) Describe the proposal/policy and the outcomes/benefits you are hoping to achieve The objective of this Policy is to safeguard the confidentiality, integrity and availability of information, information systems, applications hosted or managed within SCW networks from internal or external threats.
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: **Paul Lambert – Senior Technical Consultant**	Date completed: **08-06-2023** 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