South Central Ambulance Service
NHS Foundation Trust

Information and Security Governance Policy

V1.0

December 2021

South Central Ambulance Service NHS Foundation Trust
Unit 7 & 8, Talisman Business Centre, Talisman Road, Bicester, Oxfordshire, OX26 6HR

THIS IS A CONTROLLED DOCUMENT

This document is uncontrolled when downloaded or printed.

Document Information

Document Title	Information and Security Governance Policy
Version	V1.0 - APPROVED
Author	Simon Lacey
Intended Audience	Information Security and Governance Professionals, Human Resources
Owner	Director of Finance – Senior Information Risk Owner (SIRO)
Ratified by	Trust Board
Approved by	Trust Executive Team
Approval date	5th October 2021
Issue date	10th December 2021
To be Review By	December 2023

Related Documents

Title	Owner
Digital Strategy	Director of Digital
Freedom to Speak Up (Whistleblowing) policy & process	Freedom to Speak Up Guardian
Data and Information Quality Policy	Assistant Director for Business Information

Helpful Contacts

Team	How they can help you	Email	Telephone
Information Security and Governance Team	Most aspects of this policy	Mark.Northcott@scas.nhs.uk	01869 365131
Information Security and Governance Team	Most aspects of this policy	ISGTeam@scas.nhs.uk	
Business Intelligence	With data quality aspects of this policy	simon.mortimore@scas.nhs.uk	+ 44 77 68 39 29 04

Contents

1. Introduction

Our governance and privacy processes allow us to protect information and manage information risk consistently, whilst also complying with the legal framework.

To this end, this policy is a key foundation in how we function and use information within the Trust.

This policy allows us to protect both information and information systems regarding their:

Confidentiality	Protecting information so that it is not made available or disclosed to unauthorised individuals, entities, or processes.
Integrity	Preventing information and data from being modified in an unauthorised or undetected manner.
Availability	Ensuring information and system are available, when needed.

This policy supports our digital strategy.

2. Scope of this policy

This policy applies to all aspects governance and privacy, including the Freedom of Information Act, Data Protection Act, risk management, etc. and is written with governance and security professionals in mind.

Each control has a defined control owner, who is responsible for identifying all relevant stakeholders and subject matter experts to support these controls.

3. Training

This policy is supported by the information governance and security mandatory training, which ensures that all staff reach a minimum baseline of understanding so that they can comply with the controls set out within this policy.

If you feel you have had insufficient training to allow you to discharge your responsibilities securely, you must inform your line manager, who will support you in sourcing training appropriate to your needs.

4. Policy Concessions

If it is not possible to meet the requirements of a policy control, then a formal concession must be sought from Information Security and Governance Team.

Concessions require a formal risk assessment and are time limited and discretionary.

In all cases where a concession is granted, compensatory controls must be identified and monitored for effectiveness.

5. Sanction

Failure to comply with our policies or discharge the responsibilities defined within them may lead to disciplinary action in line with the Trust's Disciplinary & Conduct Policy.

6. Definitions and Abbreviations

We maintain a standard set of definitions and abbreviations for our information governance and security policies. These can be found on our [LINK] intranet.

7. Equality Impact Assessment

This policy will be applied fairly to all employees regardless of race, ethnic or national origin, colour or nationality; gender (including marital status); age; disability; sexual orientation; religion or belief; length of service, whether full or part-time or employed under a permanent or a fixed-term contract or any other relevant factor.

By committing to a policy encouraging equality of opportunity and diversity, the Trust values differences between members of the community and within its existing workforce, and actively seeks to benefit from their differing skills, knowledge, and experiences in order to provide an exemplary healthcare service. The Trust is committed to promoting equality and diversity best practice both within the workforce and in any other area where it has influence.

Where there are barriers to understanding, e.g., an employee has difficulty in reading or writing or where English is not their first language additional support will be put in place wherever necessary to ensure that the process to be followed is understood and that the employee is not disadvantaged at any stage in the procedure. Further information on the support available can be sought from the Human Resources Department.

Employees exercising their rights and entitlements under the regulations will suffer no detriment as a result.

The equality impact assessment can be found [LINK] here.

8. Roles and Responsibilities

We expect all our staff to work to the highest standards of information security and governance, we are all responsible for discharging our responsibilities securely and seeking assistance when we are not sure how to proceed.

Further information can be found [LINK] here, including specialist information security and governance roles and their responsibilities.

9. Policy Feedback

We welcome feedback on this policy, controls contained within it and ways in which we can make this document more impactful. Please send feedback to the Head of Information Security and Governance.

10. Information Governance

The South Central Ambulance Service NHS Foundation Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information. The Trust also recognises the need to share patient information with other health and social care organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality, most efficient, health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes. There are 4 key interlinked strands to information governance:

- Openness
- Legal compliance
- Information security
- Quality assurance

Clause 10.1

Policy Control
Openness

- Non-confidential information on the Trust and its services should be available to the public through a variety of media.

- The Trust will establish and maintain policies to ensure compliance with the Freedom of Information Act.
- The Trust will undertake or commission annual assessments and audits of its policies and arrangements for openness.
- Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients.
- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.
- The Trust will have clear procedures and arrangements for handling queries from patients and the public.

Clause 10.2

Policy Control
Legal Compliance

- The Trust regards all identifiable personal information relating to patients as confidential.
- The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements.
- The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- The Trust will establish and maintain policies to ensure compliance with the General Data Protection Regulation (GDPR), Data Protection Act 2018 (DPA 2018), Human Rights Act and the common law of confidentiality.
- The Trust will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Children's Act and the Caldicott principles).

Clause 10.3

Policy Control
Information Security

- The Trust will establish and maintain policies for the effective and secure management of its information assets and resources.
- The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements.
- The Trust will promote effective confidentiality and security practice to its staff through policies, procedures, and training.
- The Trust will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

- Utilise the Data Security and Protection Toolkit to identify information governance issues and address weakness through formal programmes of improvement.

Clause 10.4

Policy Control
Information Quality Assurance

- The Assistant Director for Business Information Has organisational responsibility for ensuring that there is in place the appropriate governance framework to support the delivery of fit for purpose D&I quality.

11. Organisation of Information Security and Governance

Security Objective:
To establish a management framework to initiate and control the implementation and operation of information security and governance within the organisation.

Clause 11.1

Policy Control
The SIRO must define the information security functions for roles and responsibilities within SCAS and ensure they are effectively communicated.

The SIRO must define the information security responsibilities for the:

- Caldicott Guardian.
- Information Asset Owners (IAO).
- Information Asset Assistants (IAA).
- IT manager.
- Line managers.
- Staff.

Control Owner
Senior Information Risk Officer.

Clause 11.2

Policy Control
The SIRO must maintain an information security and governance group, that provides oversight of the organisation's information security and governance performance, including review of risks, achievement of objectives, audit reviews and legal compliance.

The forum must:

- Agree information security objectives, understand what will be done, what resources are required, who will be responsible, when it will be completed and how the results will be evaluated.
- Ensure information security supports business objectives.
- Set risk tolerance.
- Consider changes in external and internal issues that impact information security.
- Ensure that relevant, risk based, internal audits take place.
- Monitor non-conformities and corrective action plans.
- Monitor and measure the policy framework and its effectiveness. ▪ Review information security risks.
- Ensure that risks are managed effectively and in line with tolerance.
- Support continual improvement and maturity.
- Receive feedback from stakeholders.
- Have a documented terms of reference.
- Define its membership.
- Produce an agenda.
- Produce minutes of meetings.
- Be chaired by the SIRO.
- Meet at least quarterly, more frequently, should it be required.

Control Owner
Head of Information Security and Governance.

Clause 11.3

Policy Control
The SIRO must ensure that a document management procedure is implemented, supported by a document register for all documents relevant to information security and governance.

The SIRO must ensure:

- That all documents are managed in line with the procedure.
- That the document register is kept up to date, with document owners, review dates, authors, and approvers.
- That documents are protected in line with their classification.

Control Owner
Senior Information Risk Officer.

Clause 11.4

Policy Control

The SIRO must ensure all projects formally consider information risk, security, governance, and privacy.

The SIRO must ensure that:

- Information security objectives are included in project objectives.
- Risk assessments take place and controls are identified.
- Data Protection Impact Assessments (DPIA) are conducted on all projects that significantly impact personal data.
- Information and privacy risks are included in project risk registers.
- Information security gates are included in all phases of projects.

Control Owner
Senior Information Risk Officer.

12. Asset Management

Security Objective:

- To effectively protect information assets, they must be identified, owned, and returned, as the need arises.

Clause 12.1

Policy Control
The Head of Information Security and Governance must maintain a register of information assets, in all formats.

The Head of Information Security and Governance must maintain an up to date register that records:

- Datasets, spreadsheets, etc.
- Asset purpose.
- Information Asset Owner and Information Asset Assistant.
- Classification of asset.
- Value of asset – or group of assets.
- Location of asset, both physical and virtual.
- Who has access to the asset, why and who it is shared with.
- Compliance requirements related to the asset.

Control Owner
Head of Information Security and Governance.

Clause 12.2

Policy Control
The Head of Information Security and Governance must maintain a documented procedure for the return of all information assets from individuals and third parties upon termination of employment, contract, or agreement.

The Head of Information Security and Governance must ensure that:

- Responsibility for ensuring that users return devices and assets on the last day of employment is allocated – for example, to line managers.
- Measures are in place to prevent unauthorised copying or removal of organisational assets.
- The procedure must be reviewed regularly.

Control Owner
Head of Information Security and Governance.

13. Information and Privacy Risk Management

Security Objective:
- To identify, measure and manage information and privacy risk across the organisation consistently.

Clause 13.1

Policy Control
The Head of Information Security and Governance must ensure that information and privacy risks are identified and assessed consistently, review them regularly and maintain them on a risk register.

The SIRO must:

- Use a defined risk assessment methodology, that ensures consistent, valid, and comparable results.
- Define the scope of the assessment.
- Understand the threats to the asset, including those in the supply chain.
- Define and assess vulnerabilities to the asset.
- Assess the potential resulting impact if the risk materialises.
- Assess the realistic likelihood of the risk materialising.
- Determine the risk level.
- Document the process and assessment results.

The risk assessment must consider:

- The value of the asset to the business.

- Consideration of impacts on privacy.
- The sensitivity of the data, including personal data.
- The views of relevant stakeholders and subject matter experts.
- Known incidents and near misses.
- Outputs from internal audits.
- Audit findings.
- Effectiveness of controls.
- Results of previous assessments.

Findings must be shared with the Information Security and Governance Forum and a risk owner identified.

Control Owner
Head of Information Security and Governance.

Clause 13.2

Policy Control
Risk Owners are responsible for formulating a risk treatment plan for all risks that exceed our risk tolerance.

Information Asset Owners must:

- Engage with relevant stakeholders and subject matter experts, who can advise on the most appropriate methods of risk treatment.
- Mitigate, avoid, transfer, or accept risks, in line with risk tolerance and the risk assessment.

Control Owner
Information Asset Owners.

Clause 13.3

Policy Control
Information Asset Owners must:

- Report on progress to the SIRO, through the information security and Governance Steering Group, regularly.

Control Owner
Information Asset Owners.

Clause 13.4

Policy Control
Information Asset Owners must escalate all risks that are not being managed in line with their risk treatment plans, to the SIRO.

Information Asset Owners must:

- Maintain records of discussions on risks that exceed tolerance.

Control Owners
Information Asset Owners.

14. Information Security and Governance Policy

Security Objective:

- To provide organisational direction and to support the management of information security risk, which aligns with law and regulation, whilst supporting business requirements.

Clause 14.1

Policy Control
The Head of Information Security and Governance must define, develop, and manage a framework of information security and governance policies, that consider the needs of the business, are approved by the Board, are published, and communicated to their intended audience and relevant stakeholders.

The policy framework must:

- Be developed with input from stakeholders and relevant subject matter experts.
- Align with business objectives.
- Recognise law, regulation, and best practice.
- Define their intended audience and scope.
- Define information security objectives.
- Inform readers of the concession process.
- Have a policy owner.
- State the sanction for non-compliance.
- Address the current and projected threat environment.
- Be approved by the Trust Board.

Control Owner
Head of Information Security and Governance.

Clause 14.2

Policy Control

The Head of Information Security and Governance must review the policy framework at planned intervals, or in the event of business change, changes in risk, best practice, or law.

The Head of Information Security and Governance must:

- Review policies to ensure they remain effective in supporting the business and informing the intended audience.
- Consider changes to law, regulations, and best practice.
- Consider the outputs of risk assessments, risk treatment plans, granted concessions, information security reviews, audits or incidents and known near misses.
- Consider input from stakeholders and subject matter experts.

Control Owner
Head of Information Security and Governance.

Clause 14.3

Policy Control
The Head of Information Security and Governance must maintain a documented concession authorisation process, that considers risk and compensatory controls.

The Head of Information Security and Governance must:

- Maintain a register of concession requests.
- Provide the Information Governance Steering Group (IGSG) with oversight of requests.
- Maintain a record of decisions and rationale behind them.
- Review that compensatory controls are effective.
- Ensure they are consistently applied.
- Ensure concessions are time limited.
- Consider business impact and information risk.
- Maintain a documented procedure, which is reviewed regularly.

Control Owner
Head of Information Security and Governance.

15. Legal and Regulatory Compliance

Security Objective:

- To avoid breaches of legal, statutory, regulatory of contractual obligations related to information security, governance and of any security requirements.

Clause 15.1

Policy Control
The Head of Information Security and Governance must maintain a register of applicable contractual requirements.

The Head of Information Security and Governance must:

- Identify and understand relevant contractual requirements, with input from stakeholders.
- Review the register annually, or during contract change.

Control Owner
Head of Information Security and Governance.

Clause 15.2

Policy Control
The Head of ICT Systems Support must ensure that intellectual property rights are observed.

The IT Manager must:

- Ensure purchases are made through the agreed procurement process.
- Work with stakeholders to identify ownership of licences.
- Ensure licence details are included in the asset register.
- Ensure only authorised software products are used.
- Comply with the terms of licences.
- Dispose of licences in line with the terms and conditions.

Control Owner
Head of ICT Systems.

Clause 15.3

Policy Control
The Head of Information Security and Governance must ensure that organisations records are managed effectively and securely.

The Head of Information Security and Governance must:

- Manage records in accordance with legislation, regulation, and business requirements.
- Maintain a records retention schedule.

- Maintain procedures which support records management from creation to disposal.

Control Owner
Head of Information Security and Governance.

Clause 15.4

Policy Control
The Head of Information Security and Governance must ensure that nondisclosure agreements are in place with all third parties, who may have access to organisational or client information.

The Head of Information Security and Governance must:

- Maintain a register of non-disclosure agreements.
- Ensure the agreements clearly set out responsibilities for signatories.
- Ensure that Procurement issue non-disclosure agreements, which required.

Control Owner
Head of Information Security and Governance.

16. Monitoring, Measurement, Analysis and Evaluation

Security Objective:
- To ensure the effectiveness of information security and governance and arrangements.

Clause 16.1

Policy Control
The Head of Information Security and Governance must determine what aspects of information security must be monitored, measured, and evaluated, to ensure that policy and information security objectives are being met.

The Head of Information Security and Governance must:

- Take both qualitative and quantitative measures, appropriate to the needs of the organisation.
- Complete the Data Protection and Security Toolkit annually.
- Ensure that information security performance meets the requirements of stakeholders.
- Monitor trends of performance.
- Monitor the effectiveness of Information Security performance.

- Retain information of the outputs of monitoring and measurement activities.
- Review the outputs to identify trends, which may improve our information security performance.
- Report performance to the IGSG and SIRO.

Control Owner
Head of Information Security and Governance.

17. Internal Audit

Security Objective:
- To ensure that the information security controls are functioning, as intended.

Clause 17.1

Policy Control
An internal audit of information security controls must be scoped, planned, established, and conducted annually, with a defined audit criterion and be impartial. Findings of the audit must be reported to the Information Security Steering Group and records maintained.

The internal audit must provide feedback of information security and governance, including:

- Data Security and Protection Toolkit requirements.
- Cyber Essentials +
- Legal requirements.

Control Owner
Head of Information Security and Governance.

18. Nonconformity and Corrective Action

Security Objective:
- To ensure identified non-conformities are effectively tracked and corrected.

Clause 18.1

Policy Control
All identified nonconformities must be logged, given an action owner, reviewed and its cause determined, and consideration given to where else this non-conformity may occur, with regular reports to the IGSG.

The Head of Information Security and Governance must ensure that all nonconformities:

- Are actioned by the action owner.

Control Owner
Head of Information Security and Governance

Clause 18.2

Policy Control
All nonconformities must be given an owner who will determine actions to be taken, the effectiveness of the action and will make changes to the policy framework as required.

The Head of Information Security and Governance must ensure that all nonconformities:

- Are remediated by the action owner in an agreed timescale.

Control Owner
Head of Information Security and Governance.

19. Information Security, Governance and Privacy Reviews

Security Objective:
- To ensure that information security and privacy is implemented and operated in accordance with established policy and procedures.

Clause 19.1

Policy Control
The Head of Information Security and Governance must review the organisations performance against policy and procedure regularly.

The Head of Information Security and Governance must:

- Devise a timetable for compliance reviews, which is informed by risk, incidents, concessions, non-conformities, and business requirements.
- Review against controls detailed within the information security policies.
- Review the effectiveness of corrective actions.
- Report findings back to the IGSG and Information Asset Owners.
- Maintain these findings as a record.

Control Owner
Head of Information Security and Governance.

Clause 19.2

Policy Control
The IT manager must review compliance of information systems against policy and procedure regularly.

The IT Manager must:

- Provide assurance to the Head of Information Security and Governance that controls are in place and effective.
- Seek concessions for unmet controls.
- Devise actions plans to achieve compliance, assuring the Head of
- Information Security and Governance that they will achieve compliance.

Control Owner
IT Manager.

20. Human Resources

Security Objectives:

- To ensure that we understand the competences required for roles within SCAS.
- To ensure that those that do work for us understand their responsibilities and are suitable for the roles for which they are considered.
- To ensure that those that do work for us are aware of and can fulfil their information security responsibilities.
- To protect organisational interests, during changes of employment.

Clause 20.1

Policy Control
The Head of Information Security and Governance must document the competence requirements of all roles within the organisation, which may impact information security and privacy.

The Head of Information Security and Governance must:

- Define the required information security and information governance competence for all roles within the organisation.
- Document these requirements.
- Identify, and document, gaps in existing staff knowledge and address them.
- Consider education, knowledge, and experience.

Control Owner
Head of Information Security and Governance.

Clause 20.2

Policy Control
The Head of Information Security and Governance must ensure that all those that do work for us understand the importance of information security and privacy in achieving our organisational objectives.

The Head of Information Security and Governance must:

- Promote our policies.
- Promote the role staff play in ensuring we keep information secure.
- Ensure that regular information security messages are given to staff, to keep security and privacy messages fresh and embedded in the trust.

Control Owner
Head of Information Security and Governance.

Clause 20.3

Policy Control
The Director of Human Resources must ensure that background checks are performed for all candidates prior to employment, which must be lawful and proportionate for their role within the organisation and identified information risk.

The Director of Human Resources must ensure that pre-employment checks follow national guidelines set by NHS employers.

Control Owner
Director of Human Resources.

Clause 20.4

Policy Control
The Director of Human Resources must ensure that all staff contracts include information relating to staff security, privacy, and confidentiality responsibilities.

- Contracts must include relevant clauses in relation to confidentiality and security.

Control Owner
Director of Human Resources.

Clause 20.5

Policy Control

The Head of Information Security and Governance must ensure that all staff apply information security in accordance with established information security policies and procedures.

The Head of Information Security and Governance must:

- Ensure that staff are effectively briefed on their information security roles and responsibilities.
- Ensure staff are provided with appropriate guidance and support to fulfil their information security responsibilities.
- Motivate staff to establish an environment of good information security.
- Ensure a level of awareness of information security.
- Ensure that line managers are effectively supported so that they can support employees with their information security responsibilities.
- Ensure staff maintain and improve their information security skills throughout their employment.
- Make available the Freedom to Speak Up (whistleblowing) policy and confidential process, which allows staff to freely express concerns.

Control Owner
Head of Information Security and Governance.

Clause 20.6

Policy Control
The Head of Information Security and Governance must ensure that all staff receive regular information security training, education, and awareness.

The Head of Information Security and Governance must ensure that all staff:

- Receive annual information security training, which supports the organisations information security objectives, legal compliance, commitment to information security, personal accountability, security procedures and where to find further support.
- Receive regular information security awareness messages, which are relevant to our information security objectives and support business delivery.

Control Owner
Head of Information Security and Governance.

Clause 20.7

Policy Control
The Director of Human Resources must ensure that the formal disciplinary process is sufficient for information security breaches and communicated, as required.

The Director of Human Resources must ensure:

- That the process is lawful, fair, correct, and proportionate.

Control Owner
Director of Human Resources.

Clause 20.8

Policy Control
The Director of Human Resources must ensure job descriptions include information security responsibilities, which are clearly communicated to staff and are supported by an effective joiners, movers, and leavers process.

The Director of Human Resources must ensure:

- Those changing their employment understand any enduring responsibilities, as well as new ones.
- Those leaving the Trust are aware of their ongoing, and enduring, responsibilities – including their ongoing commitment to confidentiality.

Control Owner
Director of Human Resources.

21. Data Protection Act

Security Objectives:
- To ensure that the collection, handling, processing, and sharing of personal data achieves compliance with relevant data protection law.

Clause 21.1

Policy Control
The SIRO must ensure that personal data is be processed lawfully, fairly and in a transparent manner in relation to all individuals.

The SIRO must:

- Appoint an appropriately resourced Data Protection officer (DPO), who will be responsible for maintaining data protection across the organisation and will be empowered to challenge how personal data is used and will be considered our privacy subject matter expert.

- Maintain privacy notices that clearly state what personal data we collect, who the data controller is, who we share personal data with, how personal data will be used, the legal basis for processing the personal data, how long we will hold the personal data for, how to contact the Data Protection Officer, the right to object to processing and how to contact the ICO in event of a complaint.
- Maintain a subject access request procedure and associated register to demonstrate that we are responding to requests within one month.
- Conduct Data Protection Impact Assessments (DPIA) on all new projects that may directly impact the privacy of data subjects, with oversight of the Data Protection Officer.
- DPIA's must be supported by an effective procedure.
- Maintain records of processing activities, so that we can demonstrate a full understanding of our use of personal data.
- Maintain our registration with the ICO.

Control Owner
Senior Information Risk Officer.

Clause 21.2

Policy Control
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

To achieve this principle, we will:

- Use the definitions for personal data, special category data and criminal data, as used within the Data Protection Act (2018).
- Collect data based on one of the defined legal basis.
- Where we rely upon consent to process personal data, it shall be managed by a consistent process and be informed, recorded in writing and we acknowledge that consent may be withdrawn by the data subject at any time.

Control Owner
Information Asset Owner

Clause 21.3

Policy Control
Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

To achieve this principle, we will:

- Minimise the personal data that SCAS holds and processes.

- De-identify personal data, whenever business process allows.
- Formally review both the adequacy and relevance of personal data annually, adjusting where we find that personal data is not relevant or is not adequate.
- Acknowledge the nation data opt out.

Control Owners
Information Asset Owners.

Clause 21.4

Policy Control
Information Asset Owners must ensure that personal data is accurate and, where necessary, kept up to date.

Information Asset Owners must:

- Maintain processes that assure the quality of personal data shared with us, advising the source when we find that data to be inaccurate or of poor quality.
- Maintain processes that keep personal data up to date.
- Make it easy for data subjects to ask for their personal data to be rectified or erased, when legally permissible.
- Erase or rectify data that is found to be inaccurate or out of date with 72 hours of discovery.

Control Owner
Information Asset Owner.

Clause 21.5

Policy Control
Information Asset Owners must ensure that personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Information Asset Owners must:

- Maintain a records retention schedule, that aligns with established best practice and law.
- Review the use of personal data and destroy information when it no longer supports the defined purpose for processing it.

Control Owner
Information Asset Owner.

Clause 21.6

Policy Control
Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

The Head of Information Security and Governance must:

- Establish an effective information security and privacy policy framework.
- Design processes with 'privacy by design' in mind, supporting our secure by design ethos.
- Maintain procedures that:

    a. Identify assets, which impact personal data.
    b. Map data flows of personal data.
    c. Risk assesses assets and data flows.
    d. Identify owners of assets, risks, and data.
    e. Control the disposal of personal data.
    f. Manage the transfer and sharing of personal data.
    g. Maintain subject access request procedures.
    h. Seek assurance from our third-party partners.
    i. Put in place information sharing agreements, so that we all have a common understanding of the use and protection of personal data.
    j. Manage information security incidents, learning from them to prevent reoccurrence and reporting to the ICO when necessary.
    k. Establish clear roles and responsibilities for all staff, so that they understand what is expected of them and who to contact for support.
    l. Effectively manage joiners, movers, and leavers within the organisation.
    m. Provide our staff with training and supervision, so that they can confidently handle personal information and systems the that process it.

Control Owner
Head of Information Security and Governance.

Clause 21.7

Policy Control
The Head of Information Security and Governance is responsible for demonstrating SCAS compliance with the relevant privacy law.

The Head of Information Security and Governance must ensure:

- Processes exist to demonstrate compliance.

Control Owner
Head of Information Security and Governance.

22. Freedom of Information Act

Security Objectives:

- To ensure that SCAS complies with the requirements of the Freedom of Information Act and the recognised general right of access.

Clause 22.1

Policy Control
The Head of Information Security and Governance must ensure that SCAS maintains an appropriate publication scheme, which is easily accessible to the public.

The Head of Information Security and Governance must:

- Ensure that the publication scheme meets requirements of the information commissioner's office (ICO) and is in line with the model publication scheme.
- Ensure that the publication details the formats in which information will be available, the dates or intended dates of publication and whether a charge is applicable for the supply of information.
- Monitor the effectiveness of the publication scheme.
- Review the publication scheme at least annually.

Control Owner
Head of Information Security and Governance.

Clause 22.2

Policy Control
The Head of Information Security and Governance must maintain a procedure that facilitates the Trust's compliance with the Act.

This procedure must:

- Maintain a log of requests to demonstrate compliance.
- Ensure that requests for information are processed, they must be in
- writing and include the name of the applicant, an address for correspondence, a description of the information requested, and is capable of subsequent reference.
- Provide advice and guidance to applicants, in accordance with the Code of Practice.
- Confirm or deny that the information the applicant is seeking is held by the Trust.

- Identify when the applicant should be contacted for further information to progress the request.
- Support the identification and application of applicable exemptions.
- Include when, and how, to apply fees notices.
- Allow the Trust to respond within 20 working days of receiving the request. ▪ Define the criteria for refusal of requests.
- Define the criteria for transferring requests.
- Define the considerations for third party disclosure.
- Define how to handle complaints from applicants.
- Review regularly.

Control Owner
Head of Information Security and Governance.

Clause 22.3

Policy Control
The Head of Information Security and Governance must report to the Information Security and Governance Steering Group on the Trust's performance against the Freedom of Information Act regularly.

The Head of Information Security and Governance must report on:

- Performance against timescales.
- Application of exemptions.
- Complaints from applicants.
- Performance of the publication scheme.

Control Owner
Head of Information Security and Governance.

23. Record Management

Security Objectives:
- To ensure that SCAS proactively manages its records throughout their lifecycle, from creation to disposal.

Clause 23.1

Policy Control
The Head of Information Security and Governance must maintain procedures that effectively support records throughout their lifecycle, from creation to disposal.

The Head of Information Security and Governance must ensure the procedures include:

- Establishing the reason for the records creation.
- Defining the quality of records.
- How records are stored and maintained.
- When records should be disposed of – aligning with the NHS Record Management Code of Practice.
- Any relevant law considerations – such as GDPR.
- How records should be disposed of and who may authorise disposal.

Control Owner
Head of Information Security and Governance.

24. Caldicott Guardian

Security Objectives:
- To ensure that SCAS handles personal information is used legally, ethically, and appropriately and that confidentiality is maintained.

Clause 24.1

Policy Control
The Chief Executive must appoint a senior clinician to act as the Trusts Caldicott Guardian.

The Caldicott Guardian must have a formal job description, which covers the following responsibilities:

- Strategy and governance.
- Confidentiality and data protection expertise.
- Internal information processing.
- Information sharing.
- Understanding the requirements of the Caldicott Guardian's manual.

The Caldicott Guardian must work closely with the SIRO and Information Governance teams.

Control Owner
Chief Executive.

Clause 24.2

Policy Control
The Head of Information Security and Governance must work with the Caldicott Guardian and SIRO to embed the eight Caldicott Principles throughout SCAS.

The Caldicott Principles are:

Principle 1: Justify the purpose(s) for using confidential information
Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2: Use confidential information only when it is necessary
Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information
Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strict need-to-know basis
Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities
Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6: Comply with the law
Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality
Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8: Inform patients and service users about how their confidential information is used

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

Further information can be found in the Caldicott Guardian’s Manual.

Control Owner
Head of Information Security and Governance.

Annex A – Document Governance

Version History

Version	Date	Author	Description/Change Summary
V0.1-0.7	12/03/21	Simon Lacey	Draft prepared for sign off by the Digital Director.
V0.8	11/08/21	Simon Lacey	Inclusion of comments received during consultation

Review History

Version	Date	Reviewer	Role	Comments

Sources and References

The following sources, references and legislation were consulted, as part of the development of this policy. Links correct at time of publication and will be checked at next review.

Links correct at time of publication – please report broken links.
[LINK] General Data Protection Regulation (GDPR) – Data Protection Act 2018 (DPA 2018)
[LINK] Freedom of Information Act 2000
[LINK] ISO 27001
[LINK] Caldicott Guardians Manual

Stakeholder Community

The following stakeholders were consulted during the writing of this policy and their contribution is acknowledged, with thanks.

Stakeholder	Role
Director of Finance and SIRO	Accountable
Director of Digital	Responsible
Head of Information Security and Governance	Responsible
Information Governance Manager	Consulted

Annex B – Implementation and Monitoring

Implementation plan

	Action	Owner
1.	Perform a gap analysis of existing controls and devise an action plan in the process to close identified gaps.	Head of Information Security and Governance
2.	Devise relevant procedures and processes to support this policy.	Head of Information Security and Governance
3.	Ensure that procedures are in place, are being followed, and reviewed, as necessary.	Head of Information Security and Governance
4.	Develop an audit programme so that SCAS can be assured that expectations in this policy are being met.	Head of Information Security and Governance

Monitoring plan

	Action	Owner
1.	The Information Governance Steering Group is responsible for monitoring the effectiveness of this policy and will formally document its findings.	Head of Information Security and Governance
2.	Include in the internal audit plan	Head of Audit