South Central Ambulance Service NHS Foundation Trust

ACCEPTABLE USE OF INFORMATION AND TECHNOLOGY POLICY V1.0

DECEMBER 2021

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

Table of Contents

DOCUMENT INFORMATION 3
1. INTRODUCTION 4
2. SCOPE OF THIS POLICY 4
3. TRAINING 4
4. POLICY CONCESSIONS 4
5. SANCTION 5
6. DEFINITIONS AND ABBREVIATIONS 5
7. EQUALITY IMPACT ASSESSMENT 5
8. ROLES AND RESPONSIBILITIES 5
9. POLICY FEEDBACK 6
10. USING SCAS IT EQUIPMENT 6
11. USING PERSONAL IT EQUIPMENT FOR SCAS BUSINESS 8
12. USING EMAIL 8
13. USING FAX 9
14. USE OF EXTERNAL AND INTERNAL POST 10
15. USING THE TELEPHONE 10
16. WORKING REMOTELY 11
17. PERSONAL USE OF SOCIAL MEDIA 12
18. DISCLOSING PERSONAL INFORMATION 13
19. REQUESTS FOR ACCESS TO MEDICAL RECORDS AND CORPORATE INFORMATION 14
20. STAFF RESPONSIBILITIES FOR RECORDS MANAGEMENT 15

ANNEX A – DOCUMENT GOVERNANCE 17
ANNEX B – IMPLEMENTATION AND MONITORING 18
ANNEX C – DATA PROTECTION ACT PRINCIPLES 19
ANNEX D – CALDICOTT PRINCIPLES 20
ANNEX E – POLICY ACKNOWLEDGEMENT 22

Document Information

Document Title:	Acceptable Use of Information and Technology Policy
Author	Simon Lacey

Intended Audience

- All SCAS staff, including volunteers,
- temporary and agency staff
- plus, those detailed within Section 2 of this policy.

Owner	Director of Finance – Senior Information Risk Owner (SIRO)
Ratified by	Trust Board
Approved by	Trust Executive Team
Approval date	23rd November 2021
Issue date	10th December 2021
To be Review By	End of October 2023
Version	V1.0 - APPROVED

Related Documents
Digital Strategy by Director of Digital

Helpful Contacts
Information Security and Governance Team - for most aspects of this policy
Mark.Northcott@scas.nhs.uk
01869 365131
Information Governance Team for most aspects of this policy
ISGTeam@scas.nhs.uk
IT Service Desk – For reporting incidents or suspected incidents, how to use IT equipment
ICTServiceDesk@scas.nhs.uk
03001239802

1. Introduction

This policy explains the security expectations and responsibilities that we place on all our staff to protect our service users, our organisation, and the NHS.

Information and information systems are vital to SCAS and those we serve and to this end we will protect information and 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 and operational strategies.

2. Scope of this policy

This Policy applies to all those having access to information, IT systems, equipment owned or provided by the Trust including:

- Permanent and temporary staff, contractors, and agency staff.
- All those engaged in duties for the Trust, under a Letter of Authority, Honorary Contract, Letter of Access, or Work Experience programme.
- Volunteers and all Third parties such as contractors, researchers, students, or visitors. Hereafter, all the above are collectively referred to as 'Staff' or "Employees".

It applies to suppliers and third-party providers that use or have access to the Trust's IT systems and/or equipment provided by it, where identified during the procurement process.

All staff must comply with the Data Protection Act (2018) – see Annex C.

3. Training

This policy is supported by the information governance and security mandatory training, which is available on Electronic Staff Record (ESR), which ensures that all staff reach a minimum baseline of understanding so that they can comply this policy.

If you feel you have not had sufficient 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, which could include dismissal.

All staff must sign the acknowledgement form in Annex E, confirming that they have both read and understood this policy and the responsibilities it defines.

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 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 EIA can be found 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 here, including specialist information security and governance roles and their requirements.

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. Using SCAS IT Equipment

IT equipment, systems, and software, in all forms, is provided to you so that you may discharge your responsibilities in an effective and efficient manner.

Support and advice are available from your line manager, if you are unsure of any aspects of this policy.

Policy Controls:

10.1 You are responsible for your activity and communications, when using SCAS IT equipment.

- You must not engage in activity that is unlawful, or that breaches relevant SCAS policy. Unlawful conduct includes, confidentiality, anti-discrimination laws, privacy laws, intellectual property or any criminal law or conduct that may be considered indecent, offensive, obscene, or malicious, harassment or fraud – this is not an exhaustive list.
- Be aware of the Caldicott Principles.

10.2 We may monitor or record your activity, as is permitted by Law.

- Consult your line manager for details.
- We may restrict access to websites, applications, or services which we consider inappropriate for SCAS IT equipment, or where a risk may impact our business objectives, such as excessive bandwidth consumption, or websites known to contain malicious code.

10.3 Your passwords must all be unique, and you must not use the same passwords as you do for personal use.

- We require this of you, as if your personal passwords are compromised, then this may in turn, compromise SCAS systems and data.

10.4 Your passwords must remain secret to you and must be complex, not be shared, reused, or displayed to others and your smartcard must be kept safe.

- Do not share your passwords with anyone, either inside (including with line managers, ICT staff, etc.) or outside the Trust.
- You must change default passwords to your own as soon as possible.
- You must use a unique password for each device and application.
- You must select passwords that are complex and use a combination of letters, special characters, and numbers.

- You must not use common words or easily discoverable information as passwords.
- You must not re-use passwords.
- You must not write your password down (i.e., on post it notes).
- You must remove your smartcard when you are not at your desk.
- Speak to the Head of Information Security and Governance for guidance on password managers.

10.5 You are responsible for the IT equipment that SCAS issue to you.

- You must not install software, programs, or applications onto SCAS equipment under any circumstances, except iPads. All installation is undertaken by ICT.
- You must not alter configurations or attempt to any circumvent security controls.
- You must take all reasonable precautions to protect equipment that has been issued to you, including against loss, theft, or physical damage.
- You must install patches when requested by the system or by IT.
- SCAS equipment must only be used by those authorised by the Trust.
- You must not connect non-SCAS issued equipment into SCAS networks or devices.
- You must ask if you are unsure of how to securely use your SCAS equipment.

10.6 We do allow some personal use if it does not interfere with your work and does not expose SCAS to risk to our security or reputation.

- We trust you to act responsibly, when online at work.

10.7 You must report incidents and anything you feel is suspicious immediately.

- You must report loss, theft, anything that feels suspicious about your equipment, your IT functioning unusually, any strange messages, etc. to the ICT service desk and a DATIX incident raised.
- Prompt action can effectively protect both the business and colleagues.

10.8 You must not install software, nor make copies of Trust software, unless explicitly authorised to do so or you are using a Trust issued iPad.

- SCAS maintains a list of authorised software that may be installed on Trust equipment.
- Software that is not on our approved software list must be authorised by the Head of Information Security and Governance, prior to installation.

10.9 You must lock your workstation when it is not in use or is left unattended.

- This can be done using Ctrl, Alt and Delete or the Windows key and L on your keyboard or removing your smartcard.

10.10 SCAS may seek to recover any costs that it considers excessive that are associated with the use of SCAS IT equipment.

- Typically, this would be excessive personal use of data on Trust mobile phones or where we believe that negligent use has incurred costs

11. Using Personal IT Equipment for SCAS Business

We understand that staff may want to use their own IT equipment to conduct SCAS business, such as emails, note taking, phone calls, etc, which is recognised below.

Support and advice is available from your line manager or the Information Security and Governance Team, if you are unsure of any aspects of this policy.

Policy Controls:

11.1 You are permitted to access SCAS data on personal devices only when using approved applications, such as Office 365 (including Outlook, Word, etc.) and you must not screenshot any SCAS data whilst working.

- Additional applications may be added during the lifespan of this policy and will be approved on a case-by-case basis.
- Accessing SCAS data outside these approved applications is not permitted.

12. Using email

Email allows us to communicate quickly and effectively with others, however the quick nature of emails can introduce additional information security risks, including that of sending sensitive information to unintended recipients, or sending personal identifiable information insecurely.

Support and advice is available from your line manager, the Information Security and Governance Team and the IT Service desk, if you are unsure of any aspects of this policy.

Policy Controls

12.1 You are responsible for minimising patient information within confidential emails.

- Identifiers should be removed, wherever possible, for example, use an incident number, rather than patient name and address.
- Consult your line manager for guidance.

12.2 You are responsible for ensuring emails include the correct attachments and are going to the correct recipient before you send.

- Ensure that the recipient, attachments, and classifications are correct before

pressing send – think check, check, send.

- If you miss-send an email, advise your line manager immediately.

12.3 You must not send SCAS information, or personal information that refers to patients or staff, to your personal email address.

- This means that we can no longer control our information and that it may be exposed to risks we cannot accept.
- If you have need to work remotely, then you must consult your line manager, who will assess your request and ensure you have the correct equipment to work remotely, safely.

12.4 You must only open attachments or click on links that you are expecting or are from a known, trusted, source.

- Only click on a link or open an attachment if you are sure that the email is legitimate and safe.
- Be cautious when you receive unexpected emails.
- If in doubt, do not click or open the attachment and check with sender if they have contacted you, using telephone.

12.5 You must only send personal data externally via encrypted email, such as NHS.net.

- A list of secure recipient addresses and further guidance can be found here
- Consult your line manager for guidance.

12.6 You must report incidents and anything you feel is suspicious immediately.

- You must report loss, theft, anything that feels suspicious about your equipment, your IT functioning unusually, any strange messages, etc.
- Prompt action can effectively protect both the business and colleagues.

13. Using fax

Faxes have been banned by the Secretary of Health since March 2020, and the Information Commissioners Office has deemed them unsafe for personal identifiable data and must not be used.

SCAS is removing fax machines from use and existing machines must not be used for personal identifiable data, without the express permission of the Head of Information Security and Governance.

In these cases, these controls must be observed.

Policy Controls

13.1 You must contact the Information Security and Governance team for specialist advise if you have a clinical requirement to send a fax before doing so.

- Any faxes sent without prior discussion with the Information Security and Governance team will be considered a breach of this policy.

14. Use of External and Internal Post

On occasion, you may be required to send personal data and information using either internal or external post. This can put this information at risk, so it is important that we secure the transfer, using appropriate safeguards.

Support and advice is available from your line manager or the Information Security and Governance Team, if you are unsure of any aspects of this policy.

Policy Controls

14.1 You are responsible for ensuring that all post, whether internal or external, is securely packaged, sent to a named individual or post holder, and labelled as "confidential – for addressee only".

- We recommend that staff do not send personal information in internal post, unless there is no other alternative i.e. email, external post, etc.
- If internal post is the only option, then zipped locked bags must be used, with serial number tags.
- Personal information sent via post, such as patient records, etc. must be sent via a trackable method, such as recorded or registered.
- It is advisable to obtain a proof of receipt.
- All envelopes must be robust and properly sealed.

15. Using the telephone

There remain times, when providing information by telephone is appropriate, despite the other methods of information sharing we have available to us. Using the telephone may introduce risks to information, not least, you may not know who you are talking to.

This policy sets out how the telephone can be used as safely as possible.

Support and advice is available from your line manager or the Information Security and Governance Team, if you are unsure of any aspects of this policy.

Policy Controls

15.1 You are responsible for confirming the name, job title, department and

organisation requesting the information, along with the reason they are requesting it – if the requester is unknow to you, you must verify who they are.

15.2 You must take a contact telephone number, such as main switchboard, but not a mobile or direct dial number.

15.3 You must check whether the information can be shared, that there is an information sharing agreement in place, seeking advice from Information Security and Governance where necessary.

15.4 You must provide the information to the person who requested it, not leaving information on answering machines or with colleagues, unless you are sure it is safe to do so and that only the expected recipient can hear details of the call

15.5 You must record your name, date and time of disclosure, the reason for disclosing, the information sharing agreement that is in place and the name of the person who authorised it.

15.6 You must also record the recipient's name, job title, organisation, and telephone number.

16. Working Remotely

We understand that staff may, or be required, to work remotely from Trust offices. It is important that employees understand how to work with the security of information in mind. Work away from our offices includes additional information risk, that we need to manage with additional safeguards.

This section applies to all who work outside Trust offices, either regularly or on occasion.

Support and advice is available from your line manager, the Information Security and Governance Team or the IT Service Desk, if you are unsure of any aspects of this policy.

Policy Controls

16.1 You must transport and store information and devices securely.

- SCAS would prefer that papers are not removed from site, however we recognise that this is unavoidable in some cases, where papers must be secured in a locked case in transit and securely stored at home, such as in a locked cupboard.
- Devices must be secured whilst in transit, for example in a laptop bag.
- Lock devices when not in use.
- Carry the minimum amount of information you need to do your job.
- Personal identifiable data must not be taken home, unless authorised in writing by

your line manager.

16.2 Be aware of who can hear your telephone conversations.

- Be aware of your surroundings and minimise details if you must make or take calls in busy areas or in the presence of others.
- Smart devices, such as your Alexa, should be taken out of their listening mode.

16.3 Information must be secure if you work as you travel.

- Ensure others cannot read your screens or papers.
- Fit a privacy screen to your laptop to help reduce the risk of screens being read.

16.4 You must secure devices and papers when away from the office and dispose of them securely, when you have finished with them.

- Store papers in a cupboard and ensure others cannot use your IT devices, which are provided solely for your use.
- Documents containing patient identifiable information must not be stored away from the office for long periods of time.
- Documents should be returned to base as soon as is practical.
- Clinical records must be both checked out and checked back in, where such local procedures exist.
- Confidential papers must be securely disposed of, using Trust shredding facilities, when you have finished with them and never disposed of using home household waste collections or recycling.

16.5 You must not store SCAS information on any format or solution not authorised by the Trust.

- This includes personal cloud solutions, USB sticks, IT devices, your own personal computers, your own mobile phone, or other media.
- Consult your line manager for details.

16.6 You must not use public, unsecured, wi-fi to connect to SCAS IT equipment, unless Trust approved VPN solutions are used.

- Seek specialist advice and guidance from the IT department.

17. Personal Use of Social Media

We understand that staff may wish to engage with social media and are proud of working for the NHS. However social media introduces risks that we need to mitigate and help you manage your digital footprint.

This section applies to all who engage with social media in all forms and applies to use of social media both inside and outside of work. We discourage the personal use of social media whilst at work.

Support and advice is available from your line manager, information security and governance team or internal communications, if you are unsure of any aspects of this policy.

Policy Controls

17.1 You must not use your SCAS email address to register for social media, unless it is directly a requirement of your role.

- Seek guidance if you are unsure, if social media engagement is a primary function of your role.

17.2 You must not discuss SCAS confidential business on social media unless it is directly a requirement of your role.

- Discussions about our business may endanger our intellectual property or harm our reputation, undermining the trust of our clients.

17.3 You must exercise care to ensure that your online presence does not expose SCAS to increased information security risk.

- Revealing information could undermine our business objectives.
- Cyber criminals routinely search social media for information that may increase the chances of their attacks being successful – such as phishing emails.
- You may inadvertently reveal information about our business or our security arrangements that could compromise either or both.

17.4 You must not take or post photographs of our offices or locations, or of your ID badge or smartcards, unless authorised to do so.

- Details in the background can increase information risk.

17.5 You must not claim to represent SCAS on social media unless you are authorised to do so.

- Consult your line manager or communications for details.

18. Disclosing Personal Information

During your duties, you may be asked to provide personal information by the police, or the media. In both cases, it is important that the Trust is confident of the legal basis to disclose this information and we do not expect you to make that decision yourself and you must refer these requests to relevant professionals within SCAS.

Remember, a police office does not have an automatic legal right to personal information.

Support and advice is available from your line manager, the information security and governance team and the communications team.

Policy Controls

18.1 You must refer all requests for information from the Police and other third parties to the Information Security and Governance team.

- The legal framework for disclosing personal information to the Police is complex and we would like to make the right decision, using the knowledge and expertise of our Information security and governance team, rather than expecting you to make this decision yourself.

18.2 You must refer all requests for information from the media to the Communications team.

- The Communications team will then seek authorisation to release the information.

18.3 You must only disclose patient information to other employees of SCAS, if you believe they have a genuine 'need to know', such as they are involved in that patients care, etc.

- Always check the member of staff is who are claimed to be, for example by checking their staff ID.
- Do not feel pressured to release information if you feel uncertain. Your line manager will support you.
- Consult, or refer the request to, your line manager.

18.4 You must not disclose information on a patient unless there is a genuine 'need to know', a lawful basis or consent has been given.

- A 'need to know' may include for direct care or wellbeing of the patient.
- Please be aware that requests such as these may need to be handled sensitively, as it may be a time of high stress for patients and their loved ones.
- Do not feel pressured to release information if you feel uncertain. Your line manager will support you or you can seek support from our information security and governance team.

18.5 You must not extract or run reports that contain personal identifiable information, without approval from the Information Governance Team.

- The Information Governance team may be required to complete a Data Privacy Impact Assessment (DPIA) to support this use of information.
-

19. Requests for Access to Medical Records and Corporate Information

During your duties, you may be asked to provide information by the police, or the media. In both cases, it is important that the Trust is confident of the legal basis to disclose this information and we do not expect you to make that decision yourself and you must refer these requests to relevant professionals within SCAS.

Remember, a police uniform does not have an automatic legal right to personal information.

Support and advice is available from your line manager, the information security and governance team and the communications team.

Policy Controls

19.1 You must promptly, and without delay, refer all requests for either access to, or copies of, medical records to the information security and governance team.

- These requests are considered Subject Access Requests, or SARS, and are bound within a legal framework that we must comply with.
- Requests must be processed by SCAS within one month of being received within the Trust.

19.2 You must promptly refer all requests for corporate information to the information security and governance team, who will handle these under the Freedom of Information Act.

- These requests are known as Freedom of Information Act, or FOI, requests and are bound within a legal framework that we must comply with.
- Requests must be processed by SCAS within 20 working days from the day the Trust receives the request.

20. Staff Responsibilities for Records Management

Records act as our organisational memory, both at a corporate and clinical level. It is important that these records are recorded accurately, securely storage for the stored and appropriately disposed of once their status has changed.

Records can be subject to scrutiny by those outside the organisation, so we must ensure we manage our records to support this legislation quickly and effectively.

Support and advice is available from your line manager or the Information Security and Governance Team, if you are unsure of any aspects of this policy.

Policy Controls

20.1 You are responsible for the records you create, whether they are clinical or corporate. These records must be factual, consistent, and accurate, using standardised formats and template, where these are available.

Where appropriate, records must be:

- Written in plain English.
- Written as soon as possible after an event has occurred, providing current information.
- Written clearly and in such a way that the text cannot be erased.

- Written in such a way that any alterations or additions are dated, timed, and signed in such a way that the original entry can still be read clearly.
- accurately dated, timed, and signed with the signature printed alongside the first entry.
- Not include abbreviations (unless officially accepted e.g. Clinical or Medical), jargon, meaningless phrases, irrelevant speculation, and offensive subjective statements.
- Readable on any photocopies.
- Written in black ball point pen.
- Do not include the use of correction fluid.
- Where discrepancies are found they must be reported in case incorrect actions have been taken and then the corrections added once ISG and/other relevant parties are satisfied.

20.2 You must store records in line with their sensitivity and need to retrieve them.

- Staff must follow the Lifecycle policy and Trust procedures.
- Consult your line manager for details.

20.3 You must not destroy either corporate or clinical records without appropriate authorisation.

- There is a legal requirement for us to create and maintain records, which means we need to be sure that we are entitled to dispose of records at the end of its usefulness to SCAS.
- Our record retention schedule is attached in Annex C.
- A record of destruction must be maintained when records are destroyed.
- Consult your line manager for details.

Annex A – Document Governance

Version History

Version	Date	Author	Description/Change Summary
V0.1-0.8	17/03/21	Simon Lacey	Draft prepared for sign off by the Digital Director.
V0.9	22/5/21	Simon Lacey	Password controls strengthen.
V0.91	09/08/21	Simon Lacey	Feedback from consultation included.

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.

Common Law of Confidentiality
Codes of practice for handling information in health and social care
General Data Protection Regulation (GDPR) – Data Protection Act 2018 (DPA 2018)
Human Rights Act 1998
Access to Health Records Act 1990
Freedom of Information Act 2000
The Caldicott Report
Public Records Act

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 ICT	Responsible
Head of Information Security and Governance	Responsible
Information Governance Manager	Responsible
Director Human Resources	Consulted

Annex B – Implementation and Monitoring

Implementation plan

Actions owned by: Head of Information Security and Governance

1. Include all aspects of policy within the mandatory training and awareness programmes

2. Support policy with monthly, topical article within the staff newsletter

3. Schedule and deliver online ‘surgery’ for staff to ask questions and seek guidance on the contents of this policy

4. Run an awareness campaign to explain why this policy is important.

Monitoring plan

Action

1. Owned by Head of Information Security and Governance

   The Information Governance Steering Group is responsible for monitoring the effectiveness of this policy and will formally document its findings.

2. Owned by Head of Audit

   Include in the internal audit plan

3. Owned by Head of Information Security and Governance

   Compliance checks of 4 selected business areas

Annex C – Data Protection Act Principles

SCAS must comply with the requirements of the principles of Data Protection Act (2018)

Everyone responsible for using personal data must follow strict rules called data protection principles – guidance can be sought from the Information Governance Team.

They must make sure the information is:

1. used fairly, lawfully, and transparently
2. used for specified, explicit purposes
3. used in a way that is adequate, relevant, and limited to only what is necessary
4. accurate and, where necessary, kept up to date
5. kept for no longer than is necessary
6. handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction, or damage

There is stronger legal protection for more sensitive information, such as

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

Annex D – Caldicott Principles

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.

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.

3. Use the minimum necessary personal 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.

4. Access to personal 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.

5. Everyone with access to personal 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.

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.

7. The duty to share information can be 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.

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.

Annex E – Policy Acknowledgement

We need to ensure that you have read, understand and are comfortable with the contents of our Acceptable Use of Information and Technology Policy.

Some elements of this policy are a legal requirement, such as Data Protection Act 2018. Once you have read the documents below and provided you agree to the contents, please sign the declaration, which should be counter signed by your line manager.

If you either disagree with the contents of this policy or feel otherwise unable to comply, then you must inform your line manager now.

This form will form part of your employment record.

I understand and will comply the SCAS Acceptable Use of Information and Technology Policy.

PRINT NAME:

SIGNATURE:

DATE:

ON BEHALF OF SCAS
WITNESS/MANAGERS NAME:

SIGNATURE:

DATE: