Keele University Teaching Trust

NHS North Staffordshire Combined Healthcare NHS Trust

Our Ref: NG/RM/24078
Date: 6th March 2024

Nicola Griffiths
Deputy Director of Governance
North Staffordshire Combined Healthcare NHS Trust
Lawton House
Bellringer Road
Trentham
ST4 8HH

Reception: 0300 123 1535

Dear

Freedom of Information Act Request

I am writing in response to your e-mail of the 29th February 2024**.** Your request has been processed using the Trust's procedures for the disclosure of information under the Freedom of Information Act (2000).

Requested information:
Do you have a policy or procedure that covers staff working remotely from abroad on either a temporary or permanent basis? (i.e., outside the UK)?
Please could I request a copy of the relevant policies and/or procedures?

Please see Appendices 1 and 2 attached which cover the use of mobile phones, laptops, and data processing/ access outside of the UK and senior approval would be required.

All recruitment processes are based on English law and require UK right to work. All salaries are paid subject to English taxation.

If you are dissatisfied with the handling of your request, you have the right to ask for an internal review of the management of your request. Internal review requests should be submitted within two months of the date of receipt of the response to your original letter and should be addressed to: Dr Buki Adeyemo, Chief Executive, North Staffordshire Combined Healthcare Trust, Trust Headquarters, Lawton House, Bellringer Road, Trentham, ST4 8HH. If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Yours sincerely

Nicola Griffiths
Deputy Director of Governance

NHS
North Staffordshire
Combined Healthcare
NHS Trust

Mobile Devices Policy

DOCUMENT INFORMATION	
CATEGORY:	Policy
THEME:	Finance
DOCUMENT REFERENCE:	2.20
POLICY LEAD:	Chief Information officer
DIRECTOR LEAD:	Executive Director of Finance, Performance and Digital
APPROVAL DATE:	26th October 2017
APPROVAL BODY:	People and Culture Committee
BOARD RATIFICATION DATE:	9th November 2017
FINAL REVIEW DATE:	30th September 2024

This information will be completed by the Trust Secretary

Contents

Document Tracker

Version	Date	Comments
1.0		
2.0		
2.1		

1 Policy Statement

1.1 This policy and supporting procedures is intended to address the allocation and use of NHS financed mobile phones and to set out the responsibilities expected of each North Staffordshire Combined Healthcare Trust (NSCHT) employee. It describes current legislation and also provides Health and Safety guidance relating to the usage of such devices. It includes within its scope the acceptable use of:

- Standard mobile telephones (used for phone calls and texts)
- Smartphones (as above, plus email and internet access)
- Data SIMs for use in conjunction with a laptop or tablet for remote access to the Trust network for access to clinical and corporate systems.

The policy is binding on all employees of the Trust who use a NHS mobile phone.

1.2 Each member of staff issued with a Trust mobile phone must sign an agreement to comply with the terms of the Trust mobile phone policy. In the case of existing users this will be done retrospectively – see appendix 1

2 Scope

2.1 This policy applies to all users of mobile devices (whether personal or corporate) when used in connection with the organisation's business.

2.2. All users must agree to adhere to this policy before a corporate mobile device is provided or before using a personal mobile device in conjunction with the organisation's business.

3 Duties

3.1 The **Trust** commission Staffordshire and Shropshire Health Informatics Service (S&SHIS) to deal with procurement, provide training on mobile devices and assistance and user guides when problems occur.

In the event of a fault, S&SHIS need to be contacted for assistance and will try and rectify any problems. If the problem cannot be resolved remotely, the mobile device needs to be examined by the member of S&SHIS and will need to be returned to the department when it works correctly. The S&SHIS can't guarantee that data held on a mobile device is recoverable in the event of the device having a fault.

3.2 The **User** of the mobile devices is responsible for:

- Signing the Mobile Device Agreement (Appendix 1) and ensuring compliance at all times.
- To know when and where it is appropriate to have the mobile phone switched on within the Trust.
- To access their voice mail messages on a regular basis.
- Mobile phones are frequently stolen and should not be left visible or accessible on unattended desks or on view in parked cars. In circumstances following the theft of a mobile phone, the Trust will be expected to pay for the cost of any subsequent unlawful use. This will result in an unnecessary loss to the Trust and should be avoided. When not in use a Trust mobile phone should be switched

off and accessible only by input of the appropriate PIN code.

- The loss or theft of a mobile telephone must be reported immediately to the S&SHIS for the administration of the mobile phone cancellation and the user is to inform the police. Thereafter, an Incident Report form will be submitted to the user's manager.

- All faults or damage to the mobile phone must be reported promptly to the S&SHIS If the mobile telephone develops a fault within the first year this will in most circumstances, be covered by the warranty. If and faults or damage are not covered by warranty and it is shown that the fault was due to negligence by the user, the Trust reserves the right to pass any costs on to the user.

- Any change of allocation or use of the mobile phone must be reported to the S&SHIS to enable this change to be recorded in the database/register.

- The proper use, care, maintenance and safekeeping of their allocated device(s).

- Ensuring the appropriate use of mobile devices whilst conducting their work throughout the organisation.

- Ensuring that passwords are not stored with the device.

- Not interfering or compromising the encryption or passwords on the device.

- Ensuring that no data is kept on only the mobile device but is backed up into corporate systems.

- Staff leaving the Trust must return the mobile telephone to their manager who will ensure this is returned to HIS. Any use by a former member of staff will be considered unlawful and the appropriate action will be taken.

- All users are reminded of the importance of Passwords/Personal Identification Numbers (PIN) in preventing the inappropriate use of a mobile phone allocated to them or their team. Passwords or PIN numbers should be utilised to prevent access to the mobile phone network. It is recommended that default password/PIN numbers should be changed to safeguard the phone from fraudulent use.

Failure to comply with the procedure will be investigated and might lead to disciplinary action being taken

3.3 The **Line Manager** is responsible for the mobile devices used by their staff. This includes:

- Approving and agreeing the Mobile Device Form for new devices and budget.

- Informing the S&SHIS Mobile Device team of the transfer or changes and cost centres.

- Reimbursement forms.

- Security of devices.

- Ensuring that data is not held solely on the mobile device but is backed up onto the corporate systems.

- The collection of devices from leavers (in cases when devices are not returned to the S&SHIS Mobile Device team as part of the leaving process).

- Ensuring the mobile device is returned to the S&SHIS Mobile Device team when the employee is on long-term sick, maternity leave or leaves employment.

- Where a manager suspects or believes that an NHS financed mobile phone is being misused, the manager responsible for that member of staff must consider withdrawing the mobile phone, from the member of staff, or having it disconnected, pending an investigation to determine the facts.

Failure to comply with these responsibilities will be investigated and might lead to disciplinary action being taken.

4. Framework

4.1 Procurement

- Service providers – the Trust selects to use one service provider to obtain the best price/service and to reduce administration and costs. This process is managed on behalf of the Trust, by a senior manager in the Finance Department.

- Mobile telephones ordered outside the Trust's contract will not be reimbursed.

- All requisitions for mobile phones and associated equipment must be authorised by a Trust senior manager. The order is then to be placed with S&SHIS. In all cases, the Trust standard issue phone will be provided. Any phones not standard issue will only be provided on the submission of a case with an appropriate explanation for the required device which will then require approval of the Deputy Director of Finance / Chief Information Officer.

- The S&SHIS will maintain a central database, detailing the name of holder/user, the budget holder and the telephone number of each Trust financed mobile phone.

- The purchase of mobile devices will be carried out in compliance with the organisation's purchasing arrangements.

- Purchase of mobile devices can only be done through S&SHIS.

- Budget holders and managers have the authority to approve the procurement and use of mobile devices; they must sign the bottom of Mobile Device Request Form and provide the cost code to demonstrate approval. The Deputy Director of Finance has the right to veto any such request.

- A Mobile Device Request Form (see Appendix 2) must be completed in all cases and should be forwarded to the employees Line Manager, in the first instance, to sign and then S&SHIS to action.

- It is the responsibility of each Budget Holder to ensure that adequate provision is made in the annual estimates to cover the cost of all line and call charges relating to mobile devices issued within their departments. The current costs can be obtained from S&SHIS.

- All costs for the purchase of mobile devices will be charged to the appropriate departmental budget code.

- All costs for the use of mobile devices is a revenue charge and will be charged to the appropriate departmental budget.

- Replacement or repair of damaged devices due to misuse are chargeable to the

Budget Holder.

4.2 **Allocation**

- Members of staff who have a mobile telephone allocated to them due to the nature of their employment within the Trust must comply with the Trust's mobile phone policy and to sign the Trust's conditions of agreement form – Appendix 1.

- Pool Phones: - For a group of staff who provide an on-call (or similar) service where one mobile phone is allocated to the team (to be shared appropriately within the team). The team leader is responsible for ensuring the mobile phone's appropriate use. It is recommended that a log be kept detailing who had use of the phone and on what date, this will provide an audit trail detailing the use of that phone. With this type of phone, it is recommended that there is no personal use, except in an emergency.

- The allocation of a mobile phone needs to be supported by both:

    - The budget manager against whose budget the charges will be made.

- All applications for the allocation of a mobile phone must be submitted in writing by the intended user/applicant, using the attached pro-forma (Appendix 2). The application must outline the appropriate reason for its allocation. The budget holder of the department against whose account the mobile phone will be charged must formally approve the application.

- On receipt of a mobile phone, the individual (applicant/user) will be asked to sign a declaration (see Appendix 1) acknowledging receipt of the telephone and agreeing to abide by the instructions laid out in the policy, or be liable for disciplinary action should the user fail to do so.

- Where a mobile phone is allocated to a member of staff who is on long term sick leave or some other prolonged absence from their NHS duties, then the manager responsible for that member of staff must consider re-allocating the mobile phone, to make best use of resources

- The following criteria have been developed to support managers determine which members of staff should be allocated a mobile phone.

- A standard mobile phone will be issued on a permanent basis if:
    - The member of staff has to be contactable at all times and at short notice and their role requires them to be away from their desk for the majority of their working hours.
    - The member of staff has to spend a significant amount of time travelling in the course of their work, this would include regular travelling (e.g. between Trust sites, visits to other sites or service users).
    - A risk assessment of their role recommends a phone (e.g. a lone worker)

- A smartphone will be issued if in addition to criteria outlined a member of staff needs to respond to their emails and access their diary within one working day. If a member of staff has other mobile devices from which they can access the internet a smartphone may not be necessary.

- In all cases, the Trust standard issue phone will be provided. Any phones not standard issue will only be provided on the submission of a case with an appropriate explanation for the required device which will then require approval of the Deputy Director of Finance / Chief Information Officer.

- Sim cards must NOT be swapped between devices as the mobile number associated with that device is matched to the IMEI number of the handset/computer. If this is required it will be done by S&SHIS.

5 Implementation and Monitoring

5.1 Monitoring

- The Trust considers it a management responsibility to monitor the use of mobile phones allocated to members of staff for whom they have a responsibility.

- Each month the finance department will recharge the monthly costs associated with the mobile phones to their budgets.

- The Trust receives detailed electronic information from its service provider on mobile phone usage. A rolling audit of the use of individual mobile phones will be undertaken by the Finance Directorate to ensure that;
    - staff members are paying for private usage

- The Trust has the ability to monitor the use of corporate devices and may request clarification on a number of items at any time. These items may include
    - Information held on the device
    - Calls made and received
    - Out of hours usage
    - Private calls
    - Long distance calls
    - High cost calls
    - Numbers called on a regular basis
    - Texts sent and received etc

- Where it is identified a device has been used excessively or inappropriately or for personal gain, it is the responsibility of the line manager to investigate in conjunction with the Deputy Director of Finance or nominated Finance representative.

- Where there is evidence that the NHS may have been defrauded, the Counter Fraud team will be informed and this could result in the individual being investigated under the Disciplinary Policy or prosecuted.

- Inappropriate use of any mobile device will be covered by the organisation's disciplinary rules, and include but is not limited to:
    - If a phone is used to harass or bully other individuals.
    - Inappropriate photographs or photographs taken without permission
    - Numerous and unsuitable text messages
    - Used to call premium rate numbers
    - Used to call additional chargeable services
    - Deliberate removal of security or encryption systems
    - Used in disruptive or inappropriate manner in breach of UK legislation etc.

5.2 Personal use

- Employees are allocated mobile devices for use in legitimate business purposes associated with the organisation.
- Staff are required to pay for the use of mobile devices for personal activities.
- Corporate devices must not be used for personal financial gain.

- Corporate devices must not be accessed by persons not directly employed by the organisation.
- Use of corporate devices by family members is not allowed.
- Use of a mobile phone applies to data, calls and text facilities.
- The Trust operate an **Opt-in** scheme for personal device usage with the employee able to select the appropriate usage band:

Personal use	Personal contribution (monthly)
No personal use	£0
Standard phone	£3.00
Smart phone	£10.00

If you expect to exceed the high use figures separate arrangements can be agreed with the Finance Department

- Random audits will be conducted to review personal usage of mobile phones and where usage it in excess of the agreed level, additional charges may be passed to the individual.

5.3 **Use of personal mobile devices**

- Staff who use their personal mobile devices for business related purposes and wish to recharge the organisation should first seek the agreement of their Line Manager before using the device and only use it after they have obtained written approval from the Information Security Manager, Chief Information Officer, SIRO or Caldicott Guardian.
- The general recommendation is that if there is a need to make a substantial amount of business related usage from personal devices staff should be issued with a corporate mobile device.
- Reimbursement of calls made on personal phones will be paid via the staff reimbursement of expenses form and on production of evidence of the calls from the mobile phone bill.
- Inappropriate use of personal mobile devices affecting the organisations staff, providers and clients will be treated under the disciplinary policy.
- Reimbursement of calls from pre-paid mobile phones will only be paid on production of a list of all business calls made and their costs.
- Reimbursement will not exceed £10 per month.
- Managers must be satisfied that the calls made were legitimate business calls.
- Staff can use Trust email on personal mobile devices under the following restrictions:
    - The S&SHIS must be made aware of this via a service desk call.
    - The user needs to set up the personal device by themselves
    - The user must cover all associated costs including software, data transfer etc.
    - Personal devices are not supported by the organisation or S&SHIS
    - The use of NHSmail needs to be in accordance with the Trusts Acceptable Use Policy at all times.
    - Private /personal calls during work time should be made with discretion and ensure that there is no impact to the performance of one's duties.

5.3 Call Barring

- All premium rate services, for example numbers beginning with 09 are barred on all the Trust's mobile phones. These facilities should only be provided on an individual basis where business need is identified. Written authority should be sought from the Deputy Director of Finance to remove this restriction.

- International roaming is disabled by default mobile devices can't be used outside the UK and should not be removed from the UK at any time. Written authority should be sought from the Deputy Director of Finance to remove this restriction for taking any corporate devices outside of the UK.

5.4 Health and Safety

- The health and safety of our staff is and always will be of prime importance to us. Up to date information on such concerns can be obtained from the Health and Safety Executive website – http://www.hse.gov.uk

- The Mobile Device policy will support other related safety policies put in place to minimise the risk to staff particularly staff working alone in the community. This policy should complement other Health and Safety policies whereby all roles should be subject to a risk assessment detailing ways to minimise risks in potential vulnerable situations.

5.5 Legal Obligations

- The organisation prohibits any member of staff to make or receive mobile phone calls or use in any way their mobile device when driving, this applies to both personal devices and mobiles supplied by the organisation when using personal vehicles or corporate vehicles.

- The organisation recognises that using a hands-free adaptation is not unlawful in the UK but the policy of this organisation is not to allow the use of mobile phones by drivers of vehicles that are moving.

- Any employee found to be using a hand-held phone or similar device whilst driving will be in breach of the organisation's policy and will be subject to investigation under the disciplinary policy and procedures of the organisation.

- An individual causing an accident whilst driving and using a mobile device will be reported to the appropriate authorities.

- Staff should be aware that since 1 December 2003 it has been illegal to use a hand held mobile phone whilst driving. Drivers must pull over to a safe location and turn the engine off before making or receiving calls, text messaging or accessing the internet.

- The Road Safety Act includes an offence of "causing or permitting" a driver to use a hand-held phone while driving. This applies to employers who will be guilty of an offence if they require or permit their staff who drive for work, to use a hand-held mobile phone while driving.
    - Staff are required to ensure that when they are driving they either:
    - Switch off their mobile devices
    - Leave the phone switched on and let the call go to voicemail
    - Ask a passenger to deal with the call

- Find a safe place to stop before turning off the engine and picking up the message(s) or returning call(s).

5.6 Policy maintenance

- This policy will be reviewed bi-annually or earlier in light of new national guidance / other significant changes.

- Compliance with this policy will be monitored through the mechanisms detailed within the Policy. Where compliance is deemed to be insufficient and the assurance provided is limited an action plan will be developed to address the gaps; progress against the action plan will be monitored at the specified group / committee.

Appendix 1

North Staffordshire Combined Healthcare NHS Trust
Policy for the Allocation and Use of Mobile Telephones Agreement

I agree to abide by the Trust's policy for mobile phones, which is published on the Trust's website for information.

I agree to the personal use a monthly deduction taken directly from my pay of;

Deduction	Cost	Confirmation (please tick)
No personal use	£0	
Standard phone	£3.00	
Smart phone	£10.00	

If exceeding this use I agree to repay the costs of all my personal use.

I acknowledge that I may be liable for costs relating to damage and/or faults due to my own negligence and any costs arising from the non–return of the mobile phone in accordance with the policy.

I understand that I may be liable to disciplinary action should I fail to comply with the policy.

Signed

Designation

Date

Mobile Number

Service Provider

Appendix 2

REQUEST FORM FOR MOBILE TELEPHONE

Mobile Telephone required and to be used by: (name of new user, service and base etc)		
Date of request:		
Please Provide reason for requirement:	The member of staff must be contactable at all times and at short notice and their role requires them to be away from their desk for the majority of their working hours.	
	The member of staff must spend a significant amount of time travelling during their work, this would include regular travelling (e.g. between Trust sites, visits to other sites or service users)	
	A risk assessment of their role recommends a phone (e.g. a lone worker)	
Smartphone	A smartphone will be issued if in addition to criteria outlined a member of staff needs to respond to their emails and access their diary within one working day. If a member of staff has other mobile devices from which they can access the internet a smartphone may not be necessary.	
Please list any other personnel who are likely to use the mobile telephone: (names and designations)		
Please identify finance code/budget available to cover mobile telephone charges:		
Authorised by manager		
Please print name		
Signature		
Budget Holder		
Signature		
Contact Telephone Number Please provide full telephone number (not extension only)		
Dated		

Note. This form should be completed in line with the Policy, Procedure, Procurement and Use of Mobile Telephone Policy. If you require assistance please call *(insert nominated officer's details)*

For General Services Completion
Date request received:
Date order placed:
Handled by (name/Signature):
Notes:

Equality Impact Assessment (EIA) Stage 1

Stage 1: Screening Assessment

Name of Policy or Service being assessed: Mobile Phone Policy

Policy Lead: David Hewitt

Person(s) responsible for completing the assessment (if not the Policy Lead:

The Equality Impact Assessment is a written record that demonstrates that the policy lead has shown *due regard* with respect to the characteristics protected by the Equality Act 2010 to the need to:-

i. **eliminate unlawful discrimination**,
ii. **advance equality of opportunity,** and
iii. **foster good relations** between persons with different characteristics

1. Is this a new or existing policy?	Existing
2. What is the aim of the policy/ service? ie. to ensure the Trust meets best practice for ….	To ensure mobile phones are allocated and used correctly
3. What is the expected outcome of the policy/ service? (e.g. objectives and purposes of the policy/ service, standards for practice)?	That mobile phones are allocated and used correctly.
4. Does this policy/ service link to others? If yes please state link:	No
5. Who is intended to benefit from the policy/ service? In what way? Eg all staff and service users	Users of mobile phones
5. How is the policy/ service to be put into practice? Who is responsible?	Acceptance of policy will be confirmed when a mobile phone is allocated.
6. How and where is information about the policy/ service publicised? Eg on the Trust intranet, and the internet/portal.	Trust Intranet
7. What regular consultation do you carry out with different communities and groups re the policy/ service?	No consultations undertaken

8. Equality Strands Are there concerns that the policy / service could have an adverse impact on:-	**Yes /No**	**If YES, please state evidence (either presumed or otherwise).** Please also include other relevant comments and considerations in relation to each protected characteristic area and this particular policy/service/ development.
• **Age** (eg consider impact on younger people/ older people)	No	
• **Disability** (remember to consider physical, mental and sensory impairments)	No	
• **Sex/Gender** (any particular impact on males, females, also consider impact on those responsible for childcare)	No	
• **Gender reassignment** (ie impact on people who identify as trans or non-binary)	No	
• **Race / ethnicity / ethnic communities / cultural groups**	No	
• **Pregnancy and maternity, including adoption** (ie impact during preganancy and the 12 months after; including for both heterosexual and same sex couples)	No	
• **Sexual Orientation** (impact on people who identify as lesbian, gay or bi – whether stated as 'out' or not)	No	
• **Marriage and/or Civil Partnership** (including heterosexual and same sex marriage)	No	
• **Religion and/or Belief** (includes those with religion and /or belief and those with none)	No	

9.	Do any differences identified above amount to discrimination and the potential for adverse impact in this policy? If YES could it still be justifiable e.g. on grounds of promoting equality of opportunity for one group? Or any other reason ie. Indirect discrimination can be justifiable sometimes when a service is being provided for a particular target group e.g. Asian women's breast screening, Gay men's sexual health clinic, gender specific services /environments	[redacted]/ No (if yes above, please add explanation/reasons)
10.	Do you think this policy / service /development specifically contributes to promoting equality, diversity and inclusion in North Staffordshire? If so, in what way? Please note any examples of good practice	No
11.	What approaches will you take to get feedback on your assessment?	Submission to Equality and Diversity Lead

In the case of a negative impact being identified above, please indicate any measures planned to mitigate against this by completing Stage 2, Full Impact Assessment as below:-

Stage 2: Full impact assessment

What is the impact?	Mitigating actions	Monitoring of actions

	Yes	No
Do you need any additional assistance to help you carry out the full assessment?		

Signed (Policy Lead Assessor) ……

Date ……..

GETTING FEEDBACK AND ADVICE

Feedback should now be sought from the Diversity and Inclusion Lead by emailing them at Diversity@northstaffs.nhs.uk

What feedback / guidance was provided?
(insert text here)

Counter-signed
(Diversity & Inclusion Lead) ……

Date ……..

COMPLETED FORMS – Please forward to the Diversity and Inclusion Lead via email: Diversity@northstaffs.nhs.uk
Telephone queries to: 0300 123 1535 ext 2814

Form POL7

North Staffordshire Combined Healthcare NHS
NHS Trust

Identification Of Training In Policies

Policy/ Procedure Title
Mobile Phone Policy
Statements related to training (extract these from the policy and paste into this section)
N/A
Please describe (or attach) brief details of the course content (eg an agenda for the session)
N/A
What is the Target group for this training (please describe staff groups as accurately as possible and indicate numbers of staff)
N/A
Please describe the frequency of the training indicating if this is once only or if updates are required
N/A
Who delivers this training (please include name and contact number)?
N/A
How is it advertised?
N/A
Approximately how many places per year are provided
.N/A
How is attendance against policy requirements monitored
N/A

Doc level: Trustwide
Code ref: 7.03

7.03 Information Security Policy

Lead executive	Chief Executive Officer
Authors details	Head of Information Governance Deputy Chief Information Officer

Type of document	Policy
Target audience	North Staffordshire Combined Healthcare NHS Trust workforce
Document purpose	This policy details how North Staffordshire Combined Healthcare NHS Trust will meet legal responsibilities in relation to Information Security.

Approval meeting	Finance and Resource Committee Trust Board	Meeting date	1st December 2022 12th January 2023
Ratification date	31st January 2023	Review date	31st January 2026

Trust documents to be read in conjunction with	
Document code	Document name
3.01	Disciplinary Procedure
4.18a & b	Risk Management Policy and Strategy
7.01	Confidentiality of Employee and Patient Records
7.02	Subject Access Request Policy
7.07	Records Management Policy
7.14	Safe Haven Policy
7.22	Registration Authority Policy

Document change history		Version	Date
What is different?	– Policy has been rewritten to simplify and make more user friendly for staff – The following policies have been incorporated in this policy and can be withdrawn on approval of this policy: • Pol 7.16 IT Assets • Pol 7.21 Information Risk • Pol 7.19 Mobile Information Handling	0.1 0.2	29.09.2022 25.10.2022
Appendices / electronic forms	– Definitions appendix added – Version control appendix added		
What is the impact of change?	– Ensuring that staff are aware of their responsibilities and the important of keeping all Trust assets safe and secure		

Training requirements	All staff are mandated to complete the online Data Security Awareness national training tool annually as well as other identified specialist training requirements dependent upon job role.

Document consultation	
Directorates	Digital

Corporate services	Corporate Governance
External agencies	

Financial resource implications	No

External references
1. Data Protection Act 2018 2. UK General Data Protection Regulations (UK GDPR) 3. ISO27001 Information Security Standard

Monitoring compliance with the processes outlined within this document	Any breaches to this policy will be recorded within the Trust's incident reporting system and will be investigated accordingly. This policy will be monitored and updated accordingly by the Data Protection Governance Steering Group

Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Less favorable / More favourable / Mixed impact**
Does this document affect one or more group(s) less or more favorably than another (see list)?		
– **Age** (e.g. consider impact on younger people/ older people)	No	
– **Disability** (remember to consider physical, mental and sensory impairments)	No	
– **Sex/Gender** (any particular M/F gender impact; also consider impact on those responsible for childcare)	No	
– **Gender identity and gender reassignment** (i.e. impact on people who identify as trans, non-binary or gender fluid)	No	
– **Race / ethnicity / ethnic communities / cultural groups** (include those with foreign language needs, including European countries, Roma/travelling communities)	No	
– **Pregnancy and maternity, including adoption** (i.e. impact during pregnancy and the 12 months after; including for both heterosexual and same sex couples)	No	
– **Sexual Orientation** (impact on people who identify as lesbian, gay or bi – whether stated as 'out' or not)	No	
– **Marriage and/or Civil Partnership** (including heterosexual and same sex marriage)	No	
– **Religion and/or Belief** (includes those with religion and /or belief and those with none)		
– **Other equality groups?** (may include groups like those living in poverty, sex workers, asylum seekers, people with substance misuse issues, prison and (ex) offending population, Roma/travelling communities, looked after children, local authority care leavers, and any other groups who may be disadvantaged in some way, who may or may not be part of the groups above equality groups)	No	

If you answered yes to any of the above, please provide details below, including evidence supporting differential experience or impact.	
Not Applicable	
If you have identified potential negative impact: - Can this impact be avoided? - What alternatives are there to achieving the document without the impact? Can the impact be reduced by taking different action?	
Not Applicable	
Do any differences identified above amount to discrimination and the potential for adverse impact in this policy?	No
If YES could it still be justifiable e.g. on grounds of promoting equality of opportunity for one group? Or any other reason	N/A
Not Applicable	
Where an adverse, negative or potentially discriminatory impact on one or more equality groups has been identified above, a full EIA should be undertaken. Please refer this to the Diversity and Inclusion Lead, together with any suggestions as to the action required to avoid or reduce this impact. For advice in relation to any aspect of completing the EIA assessment, please contact the Diversity and Inclusion Lead at Diversity@northstaffs.nhs.uk	
Was a full impact assessment required?	No
What is the level of impact?	Low

Contents

1. Introduction

The aim of information security is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the Trust.

North Staffordshire Combined Healthcare NHS Trust is committed to achieving the following Information Security and IG objectives:

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

Information security is everyone's responsibility and this policy sets out to ensure that information is protected from threats and confidence is maintained that our data is accurate and of good quality, through the use of technical developments and organisational management procedures.

2. Scope

This policy applies to the whole workforce at North Staffordshire Combined Healthcare NHS Trust including full-time and part-time staff, students, trainees, seconded, volunteers, contracted third parties and any other persons undertaking duties on behalf of the Trust.

It applies to all forms of information processed by the Trust and covers all business functions, information systems, networks, hardware, software, applications, mobile devices physical environments and relevant people who support those business functions.

Any breaches of this policy will be subject to the existing Trust Disciplinary Policy 3.01.

This policy will be referred to when dealing with other agencies in order to give clear guidance on the Trust's approach to information security but it does not represent the policies, procedures or guidelines of other agencies.

3. Definitions

Owing to the breadth and level of technical complexity of this policy, all relevant definitions may be found at Appendix 1.

4. Information Security Regulations, Standards and Principles

Information Security is defined as the preservation of confidentiality, integrity and availability of information:

Confidentiality:	Confidentiality can be defined as having another's trust or confidence, or be entrusted with secret or private affairs. We do this with the health records we hold. In addition to the specific rules, we all have to abide with the Common Law Principle of Confidentiality.
Integrity:	Integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire life cycle. Data must not be subject to unauthorised change, whether in transit, at rest or in use. Steps must be taken to ensure that unauthorised people cannot alter the data.
Availability:	Availability of information refers to ensuring that authorised parties are able to access the information when required. Information is only of value if the right people can access it at the right times.

5. Statutory Obligations

The General Data Protection Regulation (GDPR) was introduced in May 2018 and enhances the rules and obligations on those persons and organisations that process personal and special category data. Amongst those obligations are heightened information security standards. The Data Protection Act 2018 enacted GDPR into UK Law and we now refer to UKGDPR.

6. National Data Guardian Security Standards

The Trust is required to complete an online self-assessment annually; The Data Security and Protection Toolkit. This allows the Trust to measure performance against the National Data Guardian's 10 Data Security Standards.

7. Information Risk Management

Information risk is inherent in all activities and everyone working for or on behalf of the Trust continuously manages information risk.

Information risk management is an essential element of broader information governance and is an integral part of good management practice. The intent is to embed information risk management in a very practical way into business processes and functions.

It should be noted that this policy complements and does not supersede the Trusts Risk Management Policy and Strategy documents.

7.1 Information Risk Management Roles

To manage information risks, the following key roles have been identified:

- Senior Information Risk Owner (SIRO)
- Chief Information Officer/Deputy Chief Information Officer
- Head of Information Governance/Data Protection Officer
- Information Asset Owner (IAO)
- Information Asset Administrator (IAA)

8. Information Asset Management

8.1 Major information assets are those that are central to the efficient running of business critical functions for the Trust, ie patient, finance and personnel management processes. There are four main categories of information assets:

- **Information, Software and Hardware**

  Databases, system documentation and procedures, archive media, application programs, systems, development tools and utilities including:

  - Digital or hard copy patient health records (including those concerning all specialties and GP medical records)
  - Digital or hard copy administrative information (including, for example, HR, estates, corporate planning, supplies ordering, financial and accounting records)
  - Digital or printed x-rays, photographs, slides and imaging records, outputs and images
  - Digital media (including, for example, data tapes, CD-ROMs, DVDs, USB disk drives, removable memory sticks, mobile phones and other internal and external media compatible with NHS information systems)
  - Computerised records, including those that are processed in networked, mobile or standalone systems
  - Email, text and other message types such as eFax solutions

  Where a data protection impact assessment (DPIA) identifies that an asset is of sufficient criticality to the Trust, it may require that dedicated staff are appointed to assist in its management, e.g. an information asset owner (IAO) and whether additional business continuity (BCP) or disaster recovery (DR) plans are required (done in conjunction with Staffordshire & Shropshire Health Informatics Service (SSHIS)).

  SSHIS maintain an IT hardware and software register which details assets based on their location. Staff should not move any IT equipment without notifying SSHIS.

  The procedure for purchasing hardware and software can be found on the Trust intranet. This procedure must be followed to ensure that everything is paid for and therefore legal. The introduction/installation and/use of unauthorised hardware/software on Trust sites or Trust owned assets is a disciplinary offence.

  Object and source code for system software will be securely stored when not in use by the developer. Developers must not have access to modify program files that actually run in production. Changes made by developers must be implemented into production by technical staff. Unless access is routed through an application interface, no developer will have more than read access to production data.

Furthermore, any changes to production applications must follow the change management process. Developers must at least perform unit testing. Final testing must be performed by the clinical systems team or the target user population.

SSHIS maintain a Definitive Software Library (DSL) that contains the authorised version of all software in use. Only authorised software will be accepted into the DSL. Access to the library is strictly controlled.

SSHIS will carry out a reconciliation of software licenses at not less than 12 monthly intervals to verify that the number of licenses held matches the number of equivalent software installations. The results of the software audit will be made available to Trust managers and all anomalies investigated and corrected.

Other than access to electronic mail via Outlook Web Access (https://mail.northstaffs.nhs.uk), or access using secure authentication (Remote Access Service), staff must not process or store Trust information on their own equipment.

- **Physical**

  This includes infrastructure, equipment, furniture and accommodation used for data processing. No physical asset that is capable of holding information may be purchased outside of Trust procurement procedures.

- **Utilities and Services**

  This includes computing and communications, heating, lighting, power, air conditioning used for processing data. Local responsibility for the asset may be delegated to the Departmental Manager working in the relevant service area.

- **People**

  This includes people and their qualifications, skills and experience in the use of information systems. Each owner is responsible for ensuring that new and existing people are correctly skilled to perform their duties.

8.2 Disposal of IT Hardware and Related Media

Many IT components are highly toxic, releasing arsenic, bromine, cadmium, lead, mercury and other chemicals into the environment if not treated properly before being dumped in landfill sites.

The Waste Electrical and Electronic Equipment Directive (WEEE Directive) aims to minimise the impact of electrical and electronic goods on the environment, by increasing re-use and recycling and reducing the amount going to landfill. The UK Regulations implementing the WEEE Directive came into force in January 2007. All IT equipment must be disposed of in accordance with this Directive.

To minimise the risk of data being lost all magnetic media including hard drives will be physically destroyed.

For the purposes of this policy, IT hardware and related media **includes**:

- The personal computer (also referred to as CPU, base unit / tower / desktop / laptop etc.)
- Monitor, printer, keyboard, mouse and other peripheral devices
- Magnetic media such as hard disk drives, CDs, DVDs, tapes, USB Memory Sticks
- Photocopiers
- Projectors
- Jayex boards
- Telephone equipment

SSHIS will arrange for the safe/secure disposal of all IT hardware and related media. Any costs associated with this process are to be paid for by the budget holder responsible for the equipment being disposed of.

8.3 Information Classification

8.3.1 Owners and Production Information

All electronic information managed by the Trust must have an Information Asset Owner. Production information is information routinely used to accomplish business objectives. Owners should be Director level and responsible for assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. There are designated members of the Trust management team who act on their behalf, and who supervise the ways in which certain types of information are used and protected.

- **RESTRICTED**—this classification applies to the most sensitive business information that is intended for use strictly within the Trust. Its unauthorised disclosure could seriously and adversely impact the Trust, its service users, its business partners, and its suppliers

- **CONFIDENTIAL**—this classification applies to less-sensitive business information that is intended for use within Trust. Its unauthorised disclosure could adversely impact the Trust or its service users, suppliers, business partners, or employees

- **PUBLIC**—this classification applies to information which has been approved by the Trust management for release to the public. By definition, there is no such thing as unauthorised disclosure of this information and it may be disseminated without potential harm

9. Information Security Incident Management

An information security incident is defined as an event, which has resulted, or could result in:

- The disclosure of confidential information to any unauthorised individual. This includes manual and computerised information
- The integrity of the system or data being put at risk
- The availability of the system or information being put at risk
- An adverse impact, for example:

- embarrassment to a patient
- embarrassment to the NHS
- legal obligation or penalty
- disruption of activities
- financial loss to the Trust
- threat to personal safety or privacy

Some examples of security incidents are:

- An IT system becoming infected with a computer virus
- A user's password becoming known to other persons and used to access systems without authorisation
- Unauthorised access to confidential information/data, i.e. smartcard left in machine to be used by another member of staff
- Theft of computer hardware or health records containing patient-identifiable information

All Information Security incidents and near misses should be reported on the Trust Incident Reporting System (Safeguard).

There are occasions where confidential information is sent to the Trust in error by other organisations. These are known as **non-incidents-confidential documents received in error**. Whilst these are not strictly speaking an incident to be added to Trust Incident Reporting System (Safeguard) as they are not our breach, we have taken the decision to monitor them.

Should we then be questioned by any authority at a later date we can show due care by behaving responsibly and notifying the senders and the Information Security Department involved.

If you receive any such information, you should notify the IG staff by email, giving the date, person/organisation and your response will be sufficient for our register.

Do not forward the mail you have received as this may result in a further breach (by our Trust).

9.1 Information Governance (IG) Investigations

GDPR Article 33 compels a Controller to report, without undue delay and, where feasible, not later than 72 hours after having become aware of it, any breaches of personal data to the supervisory authority. For the Trust, this reporting is to the ICO, via the NHS Digital (NHSD) Data Security and Protection (DSP) Toolkit.

NHSD will issue the criteria and scoring scales to determine whether an incident shall be reported or can be managed locally. The DPO will issue processes to ensure that all reported incidents are investigated and reported internally to the relevant committee and, where necessary, to the ICO.

Where an IG incident appears to require reporting to the ICO, the DPO is to consult with the SIRO and the Caldicott Guardian before making their report. A consensus of these three officers will give balance and determine if the matter should be reported.

All IG investigations and information security incidents (including cyber) reporting will be in line with the Trust's overall incident reporting processes, following the procedure outlined in the Trust's incident reporting policy.

Where IG investigations tend to relate to disciplinary matters, then all evidence is to be gathered and presented in a manner where it meets the evidential requirements of the HR investigation policy.

9.2 Systems Audits

At the discretion of the DPO, IG staff will be granted access to all or any asset to undertake audits into its use. Operational managers may request audits into any specific allegation of misuse of an information asset but IG staff are not able to run routine ongoing audits where no specific evidence exists to justify that course of action; the DPO will have the final decision in all such matters.

9.3 IT Forensic Readiness

The Trust is required to have effective availability of reliable digital evidence gathered from its information assets to allow consistent, rapid investigation of major events or incidents with minimum disruption to Trust business. This is known as IT Forensic Readiness Planning.

IG staff will use the DPIA process to identify the capability of a given asset to be able to provide digital evidence in this manner.

9.4 Seizing and Securing Computer Systems for Evidence

When it is anticipated that computer systems are likely to be required as evidence to support disciplinary or criminal investigations, then IG staff are to be approached for advice.

In all cases, the National Police Chiefs' Council's *Good Practice Guide for Digital Evidence (ACPO)* is to be followed. The latest version dated March 2012 was issued under their old name of the Association of Chief Police Officers. Under no circumstances, are staff to attempt to examine computers that are suspected to be involved in criminal activity. This includes turning on and logging on to the computer involved. Such activity may render any evidence unusable.

9.5 Business Continuity Planning and Disaster Recovery

Business Continuity Planning (BCP) and Disaster Recovery (DR) for information assets are intended to provide staff with access to business critical clinical and administrative systems at an agreed reduced level during unscheduled periods of disruption.

Business Continuity Planning may be described as the actions taken by ordinary users of information assets to respond to an unplanned disruption with a view to them being able to continue to offer a service to our patients and service users.

BCP is largely with the clinical areas although supported by digital. This is system specific – some areas have digital solutions whilst other have manual processes.

The digital team work with SSHIS to define the Recovery Time Objectives (RTO's) and Recovery Point Objectives (RPO's) to meet the Trust requirements.

DR may be described as the actions taken to SSHIS and relevant staff members to restore an information asset within an agreed timescale in case of an unplanned disruption.

DR is largely done by SSHIS through technologies agreed at board level.

9.6 BCP Testing

SSHIS is a strategic partner and works with the Trust to ensure that the BCPs are adequately tested.

SSHIS hold the Trust DR plans and documentation specific to the systems and service provided to the Trust. These are evidenced as part of the toolkit.

10. Network Structure, Configuration and Security

10.1 Overview

Network Security is vital in protecting Trust data and information, keeping shared data secure and ensuring reliable access and network performance as well as protection from cyber threats.

10.2 Network Equipment

Only Trust approved devices should be connected to the network and under no circumstances should personal equipment or devices be connected to the Trust network infrastructure. This excludes personal devices being connected to Trust supplied guest Wi-Fi or another approved network.

10.3 Physical and Environmental Security

Physical and environmental countermeasures are to be adopted to minimise the risk of a breach of security to all network resources. All Trust IT assets are to be kept under lock and key when they, or the building that they are stored in, are left unattended. This includes, when a computer is left unattended in a location where members of the public have access, e.g. consulting rooms. It is also the responsibility of each member of staff to ensure that any computer they are using is not exposed to any excessive likelihood of theft. Where such a risk exists then they are to notify their line manager; the advice of IG staff may be sought. In some cases, the use of additional security devices, e.g. security cages or cables, may be necessary.

- **Data Centre Access**
  Access to the data centre must be physically restricted

- **Facility Access**
  All network equipment (routers, switches etc) and servers located in corporate offices and in all facilities must be secured when no Trust staff or authorised contractors are present.

- **Fire Suppression Systems**
  All Server Rooms and other key ICT installations are to be risk managed to decide whether or not they have fire suppression systems installed. Where installed, the fire suppression systems are to meet, and be maintained, in accordance with the appropriate legislation.

- **Uninterruptible Power Supplies**
  Uninterruptible Power Supplies (UPS) are devices that provide battery backup when the electrical power fails or drops to an unacceptable voltage level and give protection against power surges or spikes. UPS devices provide power for a few minutes; enough to power down the computer in an orderly manner, or maintain services during brief power disruptions. They are not designed to be an alternative source of power. UPS devices are to be fitted to servers and other key network devices.

- **Air Conditioning**
  Air conditioning systems may be fitted to server and communications rooms to ensure that the temperature and humidity levels in these rooms allow the computers to work at optimum levels. The requirement for air conditioning is to be risk managed based upon the individual circumstances of each location.

- **Physical Location of Server Rooms and Key ICT Assets**
  When new server rooms or other key network assets are being planned, due consideration is to be given to minimise the risk to damage through theft, fire, flood or other natural disaster. Likewise, consideration is to be given minimising the risk from accidental or malicious damage, e.g. vehicle collision or vandalism. The financial costs of these measures are lower when incorporated into new builds when compared against upgrading existing facilities. All existing facilities are to be subject to ongoing reviews to ensure that any risks are minimised.

- **Standby Generators**

  Where appropriate, consideration should be given to providing power to essential network equipment from standby generators in order to mitigate risk of damage to data and equipment through ungraceful shutdowns.

- **Network Cabling**

  Cables are essential to the transmission of information assets and to the provision of information services, but they expose risks to the availability and confidentiality of information assets and also to continuity of business operations. These risks may arise from damage to, interception or interference with these cables. Furthermore, personnel with access to these cables may accidentally cause damage.

  Consideration should be given to protecting information assets via cables against unauthorised access, use, damage or destruction by implementing appropriate measures such as secure routing of cable, armoured conduits and placing the cables underground where feasible. Cables should be subject to inspections at regular intervals to ensure that no unauthorised device is connected to the cables. Access control procedures and measures for access to cable rooms and patch panels should be established.

- **Social Engineering**

Criminals that want to steal data may use tricks to manipulate you to give them access to valuable information such as health records, patient data or IT system information - this is called social engineering.

There are many ways a social engineer may try to get information from you – here are some examples:

- Call you and pretend to be a colleague or someone from your IT helpdesk
- Ask you to hold a door open for them
- Pretend to be a 'friend' on social media

Often a social engineer will spend weeks getting to know an organisation before trying to get physical entry or making a phone call – they may find a phone list or organisational chart and use social networking sites like LinkedIn or Facebook.

What you can do to stop social engineering

- Always be vigilant at work – using the phone, receiving unsolicited emails, using social media or walking around your office – consider what information could be valuable to a social engineer
- Never reveal your login details to anyone – SSHIS and digital colleagues will never ask you for your login details
- Challenge suspicious behaviour and ask for ID – only if it's safe to do so
- Take extra care when using websites - if you get a message that you are about to use an untrusted website, it could be a fake phishing site – these can look extremely authentic and could trick you into giving away personal information
- Red padlocks mean beware - if you see a red padlock or warning message, your connection may not be private – again take care
- Think about what information you share on social media about your work – if a criminal can find posts so can your employer which could result in disciplinary action

- **Clear Desk**

NHS employees and contractors are required to ensure that all confidential information is secure within their work area. To ensure this level of confidentiality, the following measures are to be adopted:

- Confidential information, this may include diaries, notes, post its etc. must be secured when the desk is vacated – this includes meeting rooms
- Information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day
- Drawers containing confidential information must be kept locked when not in use or when not attended
- The keys used for access to the drawer must be kept secure at all times and access can be gained if necessary by a senior member of staff
- Any confidential information such as records that may need to be used by other members of staff must be place in the relevant filing cabinet and locked
- Printouts containing confidential information should be immediately removed from the printer
- All paper confidential waste must be disposed of separately to 'standard' waste and must be stored securely in an office, ward, clinic etc until it is disposed of.

Confidential waste must be placed in appropriately marked repository bins, bags or sacks. All confidential waste must be disposed of (incinerated or shredded under supervision.

- Whiteboards containing confidential information should be erased or concealed with a shutter and lock to prevent their contents being viewed.
- Treat mass storage devices such as CDROM, DVD or USB drives as confidential and secure them in a locked drawer
- Ensure computer workstations are locked or logged off when left unattended
- Reception areas should be kept as clear as possible to avoid records being within reach/sight of any visitors to the Trust and any visitor, appointment or message books should be stored in a locked area when not in use

- **Off-Site**

  - Portable electronic equipment must be kept in the possession of a Trust employee during transportation. If such equipment is lost or stolen, the matter must be reported to your line manager and SSHIS
  - Equipment or paper files should be kept out of sight, locked away and not be left unattended
  - Where a courier service is used to transport packages containing sensitive information, tamper proof packaging will be used. Courier firms should guarantee the safe arrival of parcels and the confidentiality of any contained information
  - Portable electronic equipment must have encrypted protection against unauthorised use. Passwords for example on boot-up (when a computer is switched on), should be incorporated
  - Where the Trust has supplied any form of data device, only appropriate members of staff are authorised to access it. Any member of staff allowing access to an unauthorised person, deliberately or inadvertently may be subject to disciplinary proceedings
  - Staff may not connect any supplied equipment to any phone line, Internet connection or other computer, other than where they have been given authority and access to either the NHSnet or the Trust's network via a secure remote link. Any equipment supplied for remote access to the NHS network or the organisation must be stored securely when not in use
  - Where a system requires a PIN number and a 'security token' or Smartcard these must be stored separately
  - Staff should ensure that if they are using Trust equipment at home that their personal insurance covers them for the loss of any equipment provided by the Trust
  - Storing person identifiable data files on portable devices is discouraged. Any identifiable or sensitive data stored on portable devices should have additional protection against unauthorised access and should be removed as soon as possible. If equipment has been used on a temporary basis then all data should be removed before return
  - IT equipment must be transported in a secure, clean environment
  - Provided all policy statements above are adhered to, staff may use any supplied equipment for any type of work which would normally be done on a Trust desktop PC, including the use of confidential information, provided there is compliance with general regulations on handling and storing confidential data and Trust policies

- **Homeworkers**

- Only authorised members of staff are permitted to access NHS information in any form, on any media. Use of any information at home must be related to work purposes only. Staff must ensure the security of information within their home. Where possible it should be stored in a locked container (filing cabinet, lockable briefcase). Any person identifiable or Trust confidential information that has to be taken home must be within folders marked 'Private and Confidential' and kept secure when not in use
- Any staff who need to work from person identifiable or Trust sensitive data at home must receive formal authorisation from their senior manager. This applies whether the data is to be removed in paper or electronic form

10.4 Malicious Software and Security Patches

Malicious software (Malware) may be defined as any unauthorised software introduced onto an IT system that is intended to cause harm to that system, or the data stored on that system. Malware is commonly but not exclusively referred to as computer viruses.

They can be introduced from the internet, on email attachments or on infected removable media. In addition to Malware, the network receives a threat from junk email, also known as spam. Whilst most spam is harmless, it can contain malware that is triggered when the message or attachment is opened.

SSHIS are responsible for updating and deploying anti-malware software and security patching. This includes issuing process documents for this activity. Removal of such software is not permitted.

10.5 Data Backup and Recovery

Periodically, information stored on our computers may become unavailable for a variety of reasons, e.g. the accidental deletion of a file by a member of staff, the technical failure of a hard drive or other storage media, or infection by malware. To minimize, the risk of this loss, SSHIS will perform backups on key data.

When a member of staff needs to recover any data, they should contact the SSHIS using the SMT portal and provide as much information about the file as possible. Staff should be aware that the recovery of information cannot be guaranteed, and any email or version of an email, that has been received, created or amended, and then subsequently deleted on the same day, i.e. between backups, may not be able to be recovered. Additionally, any information that is only stored on local drives or removable media cannot be recovered.

10.6 Penetration Testing and Vulnerability Scanning

A penetration test is an authorised simulated attack on a computer system, performed to evaluate the security of the system. The test is performed to identify weaknesses (vulnerabilities), including the potential for unauthorised parties to gain access to the system's features and data, as well as strengths and enabling a full risk assessment to be completed. The Trust has at least one authorised penetration test annually; it may also include a penetration test conducted under contract of NHS Digital.

The Security Operation Centre (SOC) will run periodic internal vulnerability scans using the NESSUS tool monthly. Results of these scans will be addressed in accordance

with the risk posed to the Trust. The SOC will use the Common Vulnerability Scoring System (CVSS) and Vulnerability Priority Rating (VPR) to aid in setting patching guidelines.

10.7 Cryptography Controls

The following cryptographic controls that must be applied to Trust information:

10.7.1 General Principles

Extreme care must be taken to protect our information systems and assets to prevent unauthorised access by applying where applicable, a level of encryption to sensitive or critical information which is proportionate to the Trust's risks.

All Confidential Information transferred outside of the Trust must be encrypted prior to transfer.

All removable media, including memory sticks, must be encrypted. Pre-encrypted memory sticks are approved for use on the network.

Mobile devices (laptops, tablets, digital cameras, mobile phones, CD/DVD writers, micro SD cards, scanners – this list is not exhaustive) must be protected by encryption and accessed via password and/or PIN numbers. New mobile computing devices received by SSHIS will be encrypted during the build process and before delivery to staff.

Personal unencrypted devices will be prompted to encrypt and the process cannot be reversed. NHS devices that are not encrypted will be prompted on connection to the network – failure to follow the on-screen instructions will render the device unusable on the network.

10.7.2 Encryption of Data in Transit

Confidential information in transit either physically or electronically must always be encrypted. Data which is already in the public domain (or would be of no adverse significance if it were to be so) may be sent unencrypted.

10.7.3 Encryption of Data transferred outside of the UK

Regulatory controls for any country to which data is exported outside of the UK should be checked to ensure that cryptographic legislation is not contravened, e.g. the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Where this is proposed IG staff should be consulted for approval before the transfer or travel.

11. Storing Information

As members of staff create documents, they will have a requirement to save them. However, it is important that documents are saved in a way where they can be backed up and recovered if the original document is accidently deleted, corrupted or otherwise lost.

The most common options for storing documents are detailed below:

Location	Benefits	Risks and Restrictions
Desktops	Convenient file access. Documents are available when the computer is not connected to the network.	Documents may not be recoverable if the hard drive fails as they are not backed up. Documents are normally only available on the computer where the document is stored. Documents subject to version control may lose that control if only stored on this manner. Local hard drives must not be used to store business critical documentation that is required by multiple members of staff.
Shared network folders (X drive)	Convenient file access. Access is controlled by security policy Documents available from any computer. All documents are backed up Familiar to Staff and requires no training.	Access to the document may not be possible during network disruption.
Home (or personal) network folders (U drive) Like shared network folders but the default security permissions limit access to the account holder only. These folders are limited in size. They are to be used to store personal work-related information that other members of staff will not need to access.	Convenient file access. Access is controlled by security policy Documents available from any computer. All documents are backed up Familiar to Staff and requires no training	Access to the document may not be possible during network disruption. Owing to the security permissions, only that named member of staff can access the information in it.

Location	Benefits	Risks and Restrictions
Removable Media	Convenient file access. Documents available on any computer. Any user of the media may access the document.	Does not provide users with any security controls as any user of the media may access the document. Documents are not backed up and may not be recoverable if the media fails or is lost. Documents subject to version control may lose that control if only stored on this manner. Must not be used to store business critical documentation that is required by multiple members of staff, unless all those staff have the necessary access.
Microsoft Office365	Convenient file access Documents available on any computer which has an Internet link It is designed for collaboration and sharing documents and data in many forms. E.g. One Drive, Teams Access is controlled by security permissions Access to documents from mobile devices	Vulnerable when the network or Internet is disrupted, as access to the documents may not be possible. There are still concerns in relation to user support; training and pilot sites are on a self-support basis.

11.1 Explicit Restrictions on Storage

The following locations must not be used to store Trust data:

- Any privately-owned device (including smartphones or removable media
- Any privately controlled cloud storage or email account

12. Removable Media

This paragraph introduces a series of restrictions when using removable media, where it is appropriate they must be adhered to.

Removable media is a means to transfer data, it is not intended to be a long-term storage medium, nor is it an adequate back up device. Removable Media should only be used to transport information when other more secure means are not available.

12.1 Restrictions for Storing Confidential Information on Removable Media

In order to prevent compromise or loss of Trust information, the following mandatory restrictions will apply to the storage of confidential information on removable media:

- When information is stored on removable media it is at its highest risk of compromise. Therefore, before storing any confidential information on removable media, members of staff are to exercise their professional judgement to determine whether or not the storage is appropriate and it is the only effective means available to transfer the information. *If other more secure means exist, they must be used.*
- Confidential information must only be stored on *approved secure* removable media, or by using approved encryption software that has been provided
- Confidential information is to be *copied* onto removable media. The original version is to be stored elsewhere on an appropriate network storage folder.
- Passwords must not be written down anywhere or disclosed to members of staff who do not have a need to know the material stored thereon.
- Removable media must not be used for the bulk transfer of data off site without the permission of the Trust's DPO.

12.2 Additional Restrictions for all items of Removable Media

In order to prevent compromise or loss of Trust information, the following mandatory restrictions will apply to all items of removable media:

- When information stored on an item of removable media is no longer required, it is to be deleted from the removable media
- When removable media is taken from Trust premises and is in transit, it is to be secured on the person of the individual removing it
- When removable media is taken from Trust premises and is being held on private premises, it is to be secured under "lock and key" when not in use

- All removal media is to be afforded the same level of physical protection as the most sensitive information saved thereon
- If any item of removable media is no longer required by the Trust, it must be destroyed by approved secure means
- Any loss or theft of any item of removable media must be reported immediately to SSHIS so that the level of compromise can be assessed, and necessary efforts can be made for recovery

12.3 Connecting Removable Media

This paragraph introduces guidance for connecting removable media to our network and to computers owned by other organisations and companies.

12.3.1 Using our Removable Media on non-Trust Computers

Removable media owned by the Trust may be connected non-Trust owned computers where a legitimate professional reason exists *and* the permission of the host has been given before doing so. If a legitimate professional relationship does not exist, the removable media is not to be connected.

12.3.2 Connecting Third Party Removable Media to our Computers

Removable media owned by other companies or individuals may be connected to Trust- owned computers but only where a legitimate professional reason exists. If a legitimate professional relationship does not exist, the removable media is not to be connected.

All files are swept for viruses when they are accessed but if a third party's removable media is used on our computer and a virus alert is generated, the member of staff is to stop using the device and inform SSHIS Immediately.

12.3.3 Examples of Legitimate Professional Reasons

Whilst in all cases, the member of staff concerned will have to make the decision as to whether or not a legitimate professional reason exists; it may be defined by using the following examples:

Example A
A clinician is giving a lecture to medical students at a local university and uses a PowerPoint presentation to aid this lecture.

The clinician may connect their removable media to the university computer provided that their permission is given.

Example B
A manager is meeting with representatives from partner organisations at their premises and they need to work together on a confidential business document as part of an on-going project.

The manager may connect their removable media to the host's computer as long as the partner has a legitimate reason to see the document and their permission is given. In this example, approved secure media must be used.

Example C
A company sales representative visits Trust premises to give a presentation to several members of staff and they have a demonstration version of their product on a USB memory stick.

The representative may connect their removable media to our computer to demonstrate their product. This is a legitimate professional reason.

Example D
During a visit by colleagues from another Trust, they say that they have an electronic version of a recent research document on a memory stick. The member of our staff does not have a copy of this document that would be useful for their work.

As the document is for professional use, the memory stick may be connected to our computers in order to copy the document.

Example E
A member of staff has saved a private letter to a privately-owned memory stick and they bring it to work to print it.

As no legitimate professional reason exists, the memory stick is not to be connected to our computers.

12.4 The Procurement and Availability of Removable Media

The procurement of removable media is only to be carried out by SSHIS and, where possible, only approved secure removable media as defined by the Chief Information Officer/Deputy Chief Information Officer are to be procured.

The following secure USB memory sticks are approved for use to hold confidential information, provided that they have been issue by SSHIS:

13. Access Controls

13.1 Computer System Access Control

Line managers must ensure that only authorised staff i.e. appropriate to their role, have access to information, hardware and software. Access authorisation should be regularly reviewed, particularly when staff roles and responsibilities change.

Controls are in place to ensure that only personal with the proper authorisation and a need to know are granted access to systems and resources. These controls authenticate the identity of users and validate each user's authorisation before allowing users to access information or services on the system. Information used for authentication is protected from unauthorised access.

Portable computing equipment will only be issued to staff where there is a demonstrable need for them to capture or process information away from a fixed base. Service managers must identify and justify the use of portable computing equipment when defining and appointing to posts and must notify this requirement to SSHIS as part of new starter arrangements. Service managers must also notify the SSHIS when a subsequent role change affects the need to use portable equipment. Regardless of a

laptop's ownership, the use of any equipment outside an NHS organisation's business premises for the processing of NHS information must be authorised by the relevant Director or Head of Department.

Where the processing of NHS patient information is proposed on laptop devices additional authorisation must be obtained from the organisation's Caldicott Guardian. In exceptional situations a Senior Manager can give explicit documented approval for the use of personal identifiable or sensitive data away from the normal workplace. In this eventuality the Senior Manager is responsible for ensuring the security of such information.

Any data security incident where Trust policy and procedure has been violated by staff may be subject to formal disciplinary action under the Trust's Human Resource policy framework and, if considered sufficiently serious, may constitute grounds for dismissal.

13.2 Prevention of Misuse

Any use of Trust computer facilities for non-business or unauthorised uses without management approval will be regarded as inappropriate usage.

The Computer Misuse Act 1990 introduced three criminal offences. Staff must remember that the following offences can be enforced in a court of law:

- Unauthorised access
- Unauthorised access with intent to commit further serious offence
- Unauthorised modification of computer material

13.3 Obtaining a Network Account

It is NHS policy that all staff should have access to Electronic Mail. To use email you require a network account. You also require an account to access applications such as Lorenzo, ESR etc.

A potential new user and their line manager should complete an ***Application for Network Account Form***, available on the Intranet.

13.4 Closing a Network Account

Managers should notify SSHIS of all leavers so that their network account can be disabled. Emails are retained on a leavers Outlook account for 12 months and then permanently deleted.

13.5 Training

It is the responsibility of line managers to ensure that all staff receives appropriate training in the use of the IT systems for which they have been given access.

13.6 Remote Access Service

Remote access will be controlled through identification and two factor authentication mechanisms. No confidential information may be copied from Trust network drives to non-Trust equipment (e.g. home computers) for processing.

This service is dependent upon:

- An Trust device with membership of the appropriate security group
- A pre-installed and configured digital certificate
- A broadband connection (NHS, public or private)

The following restrictions may apply to this service:

- When at home, the provision of this service is limited by the availability of a suitable broadband service. As the availability, speed and reliability of these services are beyond the control of the Trust, the availability of the Service cannot be guaranteed
- You may connect to publicly available internet connections, even though they are not shown as secure, without permission. The service creates its own encrypted connections
- The permission of any NHS third party host, e.g. a GP surgery, must be sought before attempting to connect using their network infrastructure
- SSHIS are not responsible for resolving faults affecting third party broadband services, e.g. at a GP surgery, WIFI Hotspot or at home.
- SSHIS will not make visits to non-Trust premises, e.g. a member of staff's home.
- Out of normal business hours, faults should continue to be reported but will only be addressed if the fault is affecting the service as a whole, not just an individual member of staff
- When working in public places or domestic environments, members of staff are to ensure that unauthorised persons cannot oversee any information that is displayed on their screen

13.7 Third Party Access

Third parties will not be given access to systems or networks unless the Trust/persons in question have formal authorisation to do so. All non-NHS companies will be required to sign security and confidentiality agreements with the Trust – these must be signed before access is assigned.

When permitting access to our network the following principles will apply:

- Access will only be granted after a valid request has been evaluated by a DPIA
- When permission is granted, access rights will be assigned using the principle of 'least privilege', i.e. only granting the lowest level of access necessary for the third party to effectively do their job
- When there is any doubt over the level of access rights, the Chief Information Officer/Deputy Chief Information Officer will have the final decision as to the appropriate level
- Access rights will only be granted for the duration of the contract or period of support and will be withdrawn when they are no longer required
- All solutions must include the ability for SSHIS to end the connection without any requirement for the third party to take any given action, i.e. a unilateral kill switch

Third parties found accessing elements of the system that they are not authorised to, will be deemed a security breach and will be denied access immediately. An investigation will take place to decide the outcome.

14. Use of Email

Email is provided to staff as a business tool, but because of its potential for misuse and abuse it is necessary to have in place a range of rules / guidelines to promote acceptable use for the protection of both the user and the Trust. These rules and guidelines are based on current legislation and common-sense principles. Their purpose is:

- To ensure that email is used effectively, an understanding of how it works and of good practice and etiquette that applies to its use
- To protect the users and the Trust from the risk of legal liability as a result of email abuse
- To protect and maintain the quality of Trust information against threats via external intrusion

14.1 Long-Term Absence

If a staff member is on long-term absence (more than four weeks), their line manager should with the help of SSHIS, redirect the account to someone else within the department who has authority to manage that account. The justification of redirecting the messages should be clearly established prior to redirection. The duty of confidentiality should be impressed upon the member of staff who receives the redirected mail.

14.2 General Rules

Properly used, email can be an immense benefit to the NHS and its staff. The following rules apply to anyone using the Trust's IT systems to send and receive email and the posting of information on the Trust's Web Pages:-

- Confidential person-identifiable information should not be distributed by email unless there is a specific requirement for it. Casual disclosure of personal details of patient, employee, volunteer or contractor without just cause may be considered a breach of personal privacy as defined under the Data Protection Act
- Patient identifiable data must not be sent to a personal (non-NHS) email address without additional security such as 'encryption'. Commercial internet email services are not secure and should not be used to send person-identifiable (patient and staff), confidential material or governance classified information
- Staff must not automatically forward emails from their work email address account to a commercial email address for access at home
- If however you need to send such information see the **'Secure Email Guidance'** document on the Trust intranet for clear direction on what secure method to use
- Log in at least twice daily, if not all day, and respond to requests within a

reasonable time

- Advise people when you are not available. Use the tools within your system (i.e. Out Of Office Assistant) to notify others of your inability to read your email
- Set up a Signature with your name, organisation, telephone number, other useful contact information and a legal disclaimer
- As people may receive many email messages it is important that a subject is added to the email in order that the recipient can clearly see what the email is about. It will also assist the recipient in prioritising opening of emails
- Ensure that you are sending the email to the correct person. If in doubt, confirm their email address with them
- Use the spell checker before you send out an email
- Emails should be treated like any other correspondence and should be replied to within an acceptable time limit
- Only send emails if the content would be suitable for display on a public notice board or the Trust's publication scheme. If they cannot be displayed publicly in their current state, consider rephrasing the email or using other means of communication
- Use distribution lists with care – is it important that all addressees receive the email? Only use organisation-wide distribution lists to communicate important business information that has genuine site-wide value
- Update your email groups at regular intervals. Check for leavers or members who have moved on into another role – it may not be appropriate for them to continue to receive emails from the group and may lead to a breach of the DPA
- Type your message in lower case. Using capital letters is considered aggressive

14.3 Do's and Don'ts of Email

- Staff must not send any message which is abusive, offensive, obscene or potentially defamatory or which consists of gossip. Comments of this nature can be construed as harassment. Ensure that all statements and comments you make about people or organisations are true (*Computer Misuse Act 1990*)
- Remember that the email system is for business use. You may, however, make sensible use of it for non-business purposes. Use your common sense if you send personal messages to other members of staff via this system. Bear in mind that you should not be spending more than a minimal amount of time on matters unrelated to your work. Be aware that unauthorised and excessive use of any means of electronic communications by staff at the Trust is a disciplinary offence
- Take extreme caution when disclosing your Trust Internet email addresses to outside organisations. The addresses may be misused or sold on and as a result cause an influx of junk mail
- Do not circulate jokes; computer programmes (executable files) documents such as chain letters, celebratory greetings messages (e.g. animated Christmas cards), music, video and photographs. Circulating such material can pose

serious business and operational risks by using up excessive storage space and may infect PCs or servers with viruses

- Anonymous messages are not permitted. Do not attempt to send messages purporting to come from another individual or email account without written consent
- If you send personal messages you must take care that they cannot be confused with Trust business communications
- Do not present views on behalf of the Trust, unless you are authorised to do so
- Be mindful when deleting emails permanently, as under the Freedom of Information Act, you may need to refer back to such communications or provide as evidence in responding to Freedom of Information requests
- Do not send large attachments by email. Place large attachments in a shared location (where possible) and then send just the file path via an email. If you believe that most recipients will print the document, try to use another method of sending the hard copy
- Do not attach files to emails from unknown sources (may contain viruses). Do not open file attachments with possible virus warnings. If you suspect you received a virus by email, telephone SSHIS immediately. Do not attempt to remove the virus yourself. SSHIS will need to know what virus it is
- Keep the Inbox to a minimum and adhere to good housekeeping practices. Create a personal folder structure under different headings. Transfer email from the Inbox to the appropriate folder on regular basis
- Review saved emails every month and delete any that are no longer required. If there is an email that may be required in the future, it should be archived

14.4 IT Access to Email Messages

SSHIS do not routinely monitor individual email accounts or email messages. However, in order to maintain the availability of the email system, there may be occasions when SSHIS have to access a mailbox for maintenance and housekeeping purposes e.g. if a mailbox has reached its maximum size, staff changes etc. Such access will not be used to review the content of individual email messages.

14.5 Individuals' Rights to Access Email Messages

The Data Protection Act gives individuals the right to access any information held on them, including email messages. (*Access to Health & Employee Records Policy 7.02*). In addition, the Courts and Employment Tribunals have the power to order disclosure of emails that may be relevant to a case. This emphasises the point that emails are more than just an electronic conversation. Messages should be taken seriously and the content should be in accordance with the principles of the Data Protection Act, GDPR and the Caldicott recommendations

14.6 Malicious Communications

The Malicious Communications Act 1988 makes it illegal in England and Wales to "send or deliver letters or other articles for the purpose of causing distress or anxiety".

a) a letter, electronic communication or article of any description which conveys—

   i. a message which is indecent or grossly offensive; a threat; or

   ii. information which is false and known or believed to be false by the sender; or

b) any article or electronic communication which is, in whole or part, of an indecent or grossly offensive nature,

Is guilty of an offence if his purpose or one of his purposes, in sending it is that it should, so far as falling within paragraph (a) or (b) above, cause distress or anxiety to the recipient or to any other person to whom he intends that it or its contents or nature should be communicated.

14.7 Copyright

Email messages may contain or attach copyright work owned by a third party. If you make an electronic copy of such work you may be infringing copyright (Copyright, Patents & Designs Act 1988). It is an offence to copy any item of software without the owner's prior permission. The use of illegal or unauthorised software on a Trust computer is a breach of this policy.

16. Internet Access

All sections of this policy apply to all Internet access using any NHS resources. Violation of this section will be grounds for having access to the Internet restricted or revoked.

It is clear that Internet access can be a valuable tool to staff throughout the Trust, both within their normal work activity and as an aid to learning. Furthermore, the Internet is also a route by which to deliver information and guidance to patients and to the public.

Potential Problems

There are a vast number of sites that the Trust would not wish employees to access. We must equip ourselves with a set of security measures which will minimise the risks to our resources from external intruders and which will both deter and detect employees who access 'inappropriate' Web sites. The definition of 'inappropriate' is anything that may cause offence to other individuals. **The Trust has the ability to monitor Web sites that user's access and does so on a regular basis.** It is the responsibility of a user's line manager to give the user Internet access rights or to take those rights away.

Breaches of this policy will be brought to the attention of a user's line manager and to the appropriate senior manager.

Responsibilities of the User

It is the responsibility of all staff within the Trust to ensure that the computer systems and the data that is accessed through them are safe and secure. Staff that uses the Internet have additional responsibilities relating to security, confidentiality and inappropriate use.

Permissible Access

Access to the Internet is primarily for healthcare related purposes. That is for Trust work or for professional development and training. Reasonable personal use is permitted provided that this does not interfere with the performance of your duties and is carried out during official work breaks e.g. lunchtime or outside of core working hours. The Trust has the final decision on deciding what constitutes excessive use.

Non-Permissible Access

No member of staff is permitted to use Trust provided internet connections for any of the following:

- Using another person's account or identity to access the Internet, either with or without their permission

- Attempting to download any unauthorised software, programmes or executable files
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- Audio and/or video streaming for non-work purposes, e.g. listening to the radio via the Internet
- Disclosing any patient identifiable information, business information or other confidential information on any unauthorised web site, forum or similar site
- Placing libellous, defamatory or otherwise derogatory comments on authorised Trust or any other web forum, social network or similar sites
- Harassing or bullying other members of staff as defined by Trust policy
- Operating or managing any business other than that of the Trust, except where contractually agreed with partner organisations
- Additionally, you must not intentionally access, download, store, process, display, distribute or send material, images or pseudo-images relating to the following:

    - Fraud, illegal activities, malicious activities (including computer hacking and/or software, film or music piracy)
    - Partisan political activity, political or religious lobbying or advocacy or activities on behalf of organisations having no authorised connection with the Trust.
    - *Note: The use of Trust Internet facilities by Trade Unions or other recognised professional bodies or organisations is permitted*
    - Offensive, obscene or derogatory material that is pornographic, sexist, racist or otherwise inappropriate in nature
    - Dating, escort, gambling or similar industries
    - Sites promoting the inappropriate use of illicit drugs (except where this is specifically related to the execution of your duties)
    - Audio and/or video download or retail sites (irrespective of whether or not a fee is charged)

Unintentional Breaches of Security

If you unintentionally find yourself connected to a site that contains sexually explicit or otherwise offensive material, you must disconnect from the site immediately and inform your line manager and SSHIS.

Personal Details

It is recommended that members of staff do not disclose any of their personal details over the Internet whilst using Trust facilities. These details may include:

- Demographic information
- Banking or other financial details
- Account and associated passwords

The Trust cannot be held liable for any loss related to the disclosure of any personal details that have been wilfully compromised in such a manner.

Accessing the Internet via Mobile Devices

When staff access the Internet or World Wide Web using mobile computing devices such as SmartPhones or Tablet PCs and that access is gained using a Trust network (including wireless), an audit trail of sites visited is maintained centrally by the IT Service. When access is gained through a home broadband connection, an audit trail may remain on the device.

17. Roles and Responsibilities

Chief Executive

The Chief Executive as the Accountable Officer for the Trust has overall accountability and responsibility for information security in the Trust and is required to provide assurance through the Statement of Internal Control that all risks to the Trust, including those relating to information, are effectively managed and mitigated. Details of Serious Untoward Incidents involving data loss or confidentiality breach must also be reported in the annual report.

Senior Information Risk Owner (SIRO)

The Director of Finance is responsible to the Chief Executive for information security and is the designated Senior Information Risk Owner (SIRO), who takes ownership of the Trust's Information Risk Policy, acts as advocate for information risk on the Board and provides written advice to the Accountable Officer on the content of the Statement of Internal Control in regard to information risk.

The SIRO is also required to undertaken additional information security training relevant to their responsibilities.

Caldicott Guardian

The Caldicott Guardian is the "conscience" of the organisation, providing a focal point for patient confidentiality and information sharing issues, and advising on the options for lawful and ethical processing of information as required. The Caldicott Guardian and SIRO are both concerned with ensuring NHS data is protected and is not stored, accessed or used inappropriately. The SIRO and any organisational IAOs work closely with the Caldicott Guardian and consult him/her where appropriate when conducting information risk reviews for assets which comprise or contain patient information. In most NHS Trusts the Caldicott Guardian is the Medical Director.

The Caldicott Guardian will authorise access on key issues such as sharing information and the protection and use of patient-identifiable information. The Caldicott Guardian will also advise the Trust Board on progress and issues as they arise.

The Caldicott Guardian is also required to undertaken additional information security training relevant to their responsibilities.

Chief Information Officer/Deputy Chief Information Officer

The Information Security Manager (ISM) will be responsible to the SIRO and IAOs for the identification, delivery and management of an information risk management programme to address and manage risks to the Trusts Information Assets.

Data Protection Officer (DPO)

The Data Protection Officer interprets national guidance and legislation to develop policy, strategy and systems to ensure compliance with Information Governance Data Protection requirements and the achievement of data quality standards in line with the GDPR, providing leadership, challenge and support to achieve organisational compliance.

Information Asset Owners (IAOs)

Appropriate staff will be designated Information Asset Owners (IAOs) with responsibility for the completion and maintenance of the Trust's Information Asset Register; for completing audits of their assigned assets on an annual basis as evidence for the Data Security Protection Toolkit; for providing assurance to the SIRO that information risks within their respective directorate have been identified and recorded and that controls are in place to mitigate those risks.

The IAOs are also required to undertaken additional information security training relevant to their responsibilities.

Information Asset Administrators (IAAs)

IAOs can appoint Information Asset Administrators (IAAs) to support them in the delivery of their information risk management responsibilities for the Directorate. IAAs ensure that policies and procedures are followed, recognise actual or potential security incidents and take steps to mitigate those risks, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date.

The IAAs are also required to undertaken additional information security training relevant to their responsibilities.

Managers

Managers are responsible for ensuring that:

- Information security breaches are reported through the Trust incident reporting system (Safeguard), investigated and, where appropriate, disciplinary action taken
- Information Security breach reports are provided to the relevant committees as detailed in the Trust's risk management policy (4.18).
- All the requirements of this policy are implemented, managed and maintained in their business area
- Their staff are aware of their responsibilities and accountability for information security including the potential disciplinary actions for non-compliance and that they comply with controls that are in place
- Their staff complete information security training on an annual basis as part of their mandatory training suite

- New staff complete their Trust induction which includes an overview of information security responsibilities and controls
- Local detailed processes are developed and implemented to maintain information security
- Only approved software is used on equipment that processes information. New software, which has not been properly developed and/or properly tested, is a threat to the security of existing data. All software and hardware procurements shall take account of the Trusts security requirements. This shall specifically include the procedures and actions for handing over and testing new software. Contravention of the recommendations may be considered a disciplinary offence
- Retention periods for documents relevant to each Department/Directorate via the Trust's Records Management Policy 7.07, which includes reference to the safe destruction of documents are maintained
- System training is provided prior to users operating any clinical system, according to the access level required
- All redundant and unwanted IT hardware and related media is returned to SSHIS for safe disposal
- Staff who remove information in any form or use information in any form away from the usual Trust workplace are aware and comply with this policy
- Service Managers and internal auditors are responsible for assessing risks and ensuring that controls are being applied effectively
- SSHIS are informed if:

    - IT equipment is transferred to another area
    - Staff circumstances change as it may affect access to systems
    - New software and hardware are required
    - Prior to operating any clinical systems all potential users, including temporary/agency staff, must receive system training according to the access level required

Data Protection Steering Group

Overall responsibility for confirming whether remote access to business applications and systems is permitted away from the usual Trust workplace

Trust Chief Information Officer/Deputy Chief Information Officer

Provide assistance on implementing controls for staff members that do not work in the usual Trust workplace

Staffordshire & Shropshire Health Informatics Service (SSHIS)

The Staffordshire & Shropshire Health Informatics Service (SSHIS) will provide appropriate management information in relation to IT and IT related equipment and software.

Staff

Information security and the appropriate protection of information assets, which includes information in emails and the email system, is everyone's responsibility.

All staff are obliged to:

- Comply with this policy and support its objectives
- Complete their annual information security awareness training
- Ensure that they understand their responsibilities around information security and comply with the law
- Report information security incidents via the Trust's incident reporting system (Safeguard)
- Ensure that they do not save files that contain offensive material. To do so may constitute a serious breach of Trust security and could result in dismissal and/or criminal prosecution. The Trust is the final arbiter on what is or is not offensive material
- Ensure that data quality is maintained
- Failure to comply with this policy is a disciplinary offence
- Ensure that they do not install software onto a Trust owned device. SSHIS conduct audits of all software and if unauthorised/and or unlicensed software has been purchased, they are authorised to remove it
- Advise SSHIS if there is a suspicion that unauthorised software is present on your asset
- Ensure that anti-virus software is installed and active – contact SSHIS for advice
- Lock your computer when leaving it unattended

Staff that work away from the usual Trust workplace

In addition to the responsibilities above:

- Keep usage to a minimum in public areas
- Only access information off-site/at home for work-related purposes
- Ensure security of information within the home or off-site
- Not connect any Trust supplied equipment to any computer network other than the NHS network or the Trust's network other than by using the secure access procedure. This includes the use of Wireless Access Points often found in public buildings
- Not use patient identifiable or staff identifiable data on any equipment not provided by the Trust
- Not send patient or staff identifiable data to home (Internet) email addresses. • Keep equipment, media and files including paper locked out of sight during transit
- Ensure equipment and files are adequately packaged in transit to prevent damage or tampering
- Not dispose of any media containing sensitive/confidential information (including paper) off-site. All such information must be returned to a Trust-owned location for safe disposal

18. Monitoring and compliance

The Trust reserves the right to monitor work processes to ensure the effectiveness of the services provided. This will mean that any personal activities that any employee engages in during work time may come under scrutiny. It will respect the privacy of its employees and does not want to interfere in their personal lives but monitoring of work processes is a legitimate business interest.

Managers are expected to speak to staff of their concerns should any minor issues arise. If serious breaches are detected an investigation must take place. Where this or another policy is found to have been breached the relevant Trust procedures will be followed.

Concerns about possible fraud and or corruption should be reported to the Counter Fraud Department.

In order for the Trust to achieve good information governance practices, staff must be encouraged to recognise the importance of good governance and report any breaches or incidents to enable lessons to be learned. Staff must be provided with the necessary tools, support, knowledge and training to help them deliver their services in compliance with legislation. Ultimately a skilled workforce will have the confidence to challenge bad information governance practices, and understand how to use information legally in the right place and at the right time. This should minimise the risk of incidents occurring or recurring.

19. Review

This policy will be reviewed every two years or more frequently where the contents are affected by major internal or external changes such as:

- Changes in legislation;
- Changes in systems/technology; or
- Changing methodology.

Any updates and amendments to this Policy will be recorded in the document control section in Appendix B.

Appendix A: Definitions

Term	Description
Asset Register	Essentially a list of an organisation's assets and their condition and helps an organisation to ascertain what it owns or leases and the stock of that item.
Business Continuity	The ability of an organization to maintain essential functions during, as well as after, a disaster has occurred.
Common Law Principle of Confidentiality	Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges and is also referred to as 'judge-made' or case law. The law is applied by reference to previous cases and is said to be 'based on precedent'.
Consequence	The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain.
Data Protection Impact Assessment	A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.
Data Protection Officer	Legally accountable to the Information Commissioner's Office and responsible to the SIRO to ensure that the Trust processes its personal and special category data lawfully and its information risks are correctly managed.
Data Security and Protection Toolkit	The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian`s 10 data security standards.
Digital Certificate	Used to encrypt online data/information communications between an end-users browser and a website.
Disaster Recovery	Involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.
Freedom of Information Act	An Act of Parliament of the Parliament of the United Kingdom that creates a public "right of access" to information held by public authorities.
General Data Protection Regulation	The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area.
Hardware	Describes the physical aspects of a computer/device.
Information Asset Administrator	A term given to staff, typically within ICT, who actively support the maintenance and operation of a given information asset.
Information Asset Owner	A senior member of staff with responsibility for the management of a given information asset within their area of responsibility.
Least Privilege	Only granting the lowest level of access necessary for the third party to effectively do their job.

Term	Description
Likelihood	A qualitative description or synonym for probability or frequency.
Malicious Software	Also known as malware, is any software that does harm to the system, such as a virus or spyware.
Malicious software attacks	Also known as malware, is any software that does harm to the system, such as a virus or spyware.
National Data Guardian for Health and Care	An independent, non-regulatory, advice giving body in England sponsored by the Department of Health and Social Care.
Recovery Point Objective (RPO)	The agreed point in time before the disruption to which information should be recovered to within the RTO.
Recovery Time Objective (RTO)	Target time for services to be restored to an agreed state following disruption.
Remote Access Service	Any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices.
Risk	The chance of something happening which will have an impact upon objectives. It is measured in terms of consequence and likelihood.
Risk Assessment	The overall process of risk analysis and risk evaluation.
Risk Management	The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.
Risk Management Process	The systematic application of management policies, procedures and practices to the task of establishing the context, identifying, and analysing, evaluating, treating, monitoring and communicating risk.
Security Patching or Patch	Set of changes to a computer program or its supporting data designed to update, fix, or improve it. This includes fixing security vulnerabilities and other bugs.
Serious Incident Requiring investigation	Incident where one or more patients, staff members, visitors or member of the public experience serious or permanent harm, alleged abuse or a service provision is threatened.
Software	A set of instructions, data or programs used to operate computers and execute specific tasks. Software is a generic term used to refer to applications, scripts and programs that run on a device
Software Update(s)	An update is new, improved, or fixed software, which replaces older versions of the same software
Spam	Refers to the use of electronic messaging systems to send out unrequested or unwanted messages in bulk.
Special Category Data	Personal data is any information that relates to an identified or identifiable living individual.
Viruses	Type of malicious software that, when executed, replicates itself by modifying other computer programs and inserting its own code

Appendix B: Policy Development - Version Control

Revision History

Date	Version	Author	Revision Summary
29/09/2022	0.1	Head of Information Governance	Full rewrite of Information Security Policy incorporating IT Assets, Information Risk and Mobile Information Handling to streamline and make more transparent and available for staff
25/10/2022	0.2	Head of Information Governance	Incorporating further information around BCP/DR and Social Engineering

Reviewers

This document requires the following reviews:

Date	Version	Position
14/10/2022	0.1	Deputy Chief Information Officer
14/10/2022	0.1	Chief Information Officer
25/10/2022	0.2	Deputy Chief Information Officer

Approvers

This document requires the following approvals:

Date	Version	Name	Status
31/10/2022	V0.2	Data Protection Steering Group	Approved
		Senior Leadership Team Group	