Information Security: Acceptable Use Policy

Lead Manager	**IT Compliance Manager**
Responsible Director	**Director eHealth**
Approved By	**Information Governance Steering Group**
Date Approved	**26/02/2020**
Review Date	**26/02/2022**
Version No.	**N1.0**
Replaces Version	**1.9**

1 Document Control

1.1 Revision History

Date	Author	Version	Summary of Changes
16/10/2017	Arunava Banerjee	1.0	Initial Draft
19/12/2017	Stephen Harris	1.1	Revised
04/01/2018	Arunava Banerjee	1.2	Formatted and added new contents
16/01/2018	Stephen Harris	1.4	Updated with comments from APF
31/01/2018	Stephen Harris	1.5	Editing and changes in formatting
6/02/2018	Stephen Harris	1.6	Updated with comments from APF
12/04/2018	Stephen Harris	1.7	Updated with 8.2 AUP Topic Relationship to Other Policies, 8.3 Learning Material
08/05/2018	Arunava Banerjee	1.8	Updated with comments from APF Editing and changes in formatting Added hyperlinks to policies referred in the AUP
26/02/2019	Arunava Banerjee	1.9	Added 5.2.2 c. Use of NHS emails with non-NHS services for a corporate purpose.
28/05/2019	Stephen Harris	1.10	Expansion of 5.8 Blogging and Use of Social Media
18/10/2019	Stephen Harris	N 1.0	Policy references updated for Network Information Systems (NIS) Regulations
20/12/2019	Arunava Banerjee	N1.0	Updated References

1.2 Review and Approvals

Role/Title	Authority	Approval Date
Area Partnership Forum	Area Partnership Forum	28/05/2018
Information Governance Steering Group	Information Governance Steering Group	30/05/2018
Area Partnership Forum	Area Partnership Forum	26/02/2020
Information Governance Steering Group	Information Governance Steering Group	26/02/2020

Contents

2 Introduction

The risks to NHS Greater Glasgow and Clyde (NHSGGC) through IT security compromise are increasing as attacks increase in frequency and sophistication. The Network Information Systems (NIS) Regulations and General Data Protection Regulation (GDPR) became a legal requirement. The newly formed Scottish Health Competent Authority (CA) issued the Information Security Policy Framework 2018 which identifies the People, Technology and Process controls for NHS Scotland. This has required that NHS GGC's policies be revised. There are no changes to the behavioural components from the previous policies. In this version of the Acceptable Use Policy the references have been updated. This Acceptable Use Policy takes the behavioural components from our security policies to provide the parameters for staff behaviour. While not looking to impose restrictions that are contrary to NHSGGC's established culture of openness, trust and integrity behaviours need to change to meet the security requirements of the digital age.

The scope of computer use continues to expand and now includes desktops, laptops, tablets and smartphones. These are used to access internal and cloud hosted systems. With increasing pervasiveness of internet connectivity, access can be from NHSGGC or partner premises, patient home or public places. Each environment poses different issues which this Policy looks to clarify.

Effective security requires the combination of people, technology and process working together.

3 Purpose

The purpose of this policy is to outline the acceptable use and behaviour of all staff that are using NHSGGC computer equipment and IT Services.

4 Scope

This is a board-wide policy and applies to all users of NHSGGC IT systems.

5 Policy

5.1 General Use of Information Systems

All staff, as defined in their terms and conditions of employment need to be aware of organisational polices including Information Security. Policies are updated and amended in line with business, technology or legislative changes. Any approved amendments will be published and communicated with staff accordingly

5.1.1 Staff Responsibilities

a) All staff must read and comply with the NHSGGC Information Security Policies. Failure to observe these policies could result in investigation which may lead to disciplinary action or legal proceedings being taken against the offender.

b) Staff are, through their UserID granted access rights to IT systems at levels appropriate for their organisational role(s).

c) All individuals entrusted with access to information have a responsibility to ensure that their actions when using information systems conform with this policy

d) Each member of staff has a personal responsibility to ensure that no breaches of computer security result from their actions.

e) All staff must notify their line manager of any suspected or actual breaches of confidentiality. Line management must report to the eHealth Security Manager/Compliance Manager via the eHealth Service Desk of any suspected breaches of security arising from the actions of any member of staff.

f) If inappropriate use of any NHSGGC computer is known or suspected, then investigations will be instigated under the direction of Human Resources. This will follow the NHSGGC Disciplinary Policy and Procedure. https://www.nhsggc.org.uk/working-with-us/hr-connect/policies-and-staff-governance/policies/disciplinary-policy-procedure-overview-1/disciplinary-policy/Police or other regulatory bodies may be engaged as appropriate.

g) Staff must log out when not using the computer or ensure that it is locked and screensaver on, (using Ctrl/Alt/Del or Windows key + L) particularly in patient facing areas.

5.1.2 Line Manager's Responsibility

Management should ensure that staff are properly briefed on the content of this policy and their information security roles and responsibilities prior to being granted access to sensitive information.

a) It is the responsibility of the Line Manager to update eHealth via My Account or email to User.Provisioning@ggc.scot.nhs.uk when a member of staff

   a. Joins NHSGGC
   b. Terminates their employment

b) Staff roles change, therefore varied system access can be required. To ensure that amendments are updated, managers will notify the eHealth Service Desk about staff changes affecting computer access (e.g. job function changes/leaving department or organisation), so that accounts may be disabled, deleted, data transferred or access rights modified.

c) Managers will determine which individuals are to be given access to computer systems. The level of access to specific systems should be based on a job function need, irrespective of status. This forms Role Based Access Control.

d) Learning material is available from different sources, on-line and class room. Managers will ensure that all current and future staff are fully aware of their information security responsibilities.

e) Managers will ensure that all their staff using Trakcare, Clinical Portal, EMIS Web or Badgernet have been trained.

f) Managers will ensure that no unauthorised staff are allowed access to any of the organisation's computer systems.

g) Managers will have business continuity processes that can be implemented during unavailability of IT systems.

h) If managers believe that there is a cause to initiate an investigation into a Data Breach then they must contact a senior member of Human Resources. In the first instance, discussion and consideration of suspension of the individual/s must be undertaken to protect the Organisation and information sources. Please also refer to the NHSGGC's Data Breach Policy.

5.2 Identity and Access Management and keeping personal details up to date

Access to NHSGGC systems is dependent on user credentials, UserID and password(s). To maintain integrity of both, the IT system and its underlying databases, particularly patient records, each member of staff needs to manage their credentials and not share their password. On occasion, particularly if suspected data breach or investigation of a care episode there may be a requirement to audit the use of the UserID both in terms of searches made and records updated.

5.2.1 Password Management

a) For passwords to be an effective security measure, they should not be easy for someone to guess. Names, words, telephone numbers, dates of birth etc., should not be used. Passphrases, word splitting, incorporation of numeric and wild characters are encouraged.

b) To prevent unauthorised access to any NHSGGC system all users are responsible for ensuring that their passwords are kept secure and confidential and never disclosed even to eHealth staff.

c) Where it is necessary to write down a password for contingency reasons it should be held in a secure way or in a secure environment so that it is not accessible by anyone else e.g.as part of random notes.

d) Using someone else's UserID and password is a breach of the Computer Misuse Act. Using someone else's ID card and PIN to access the computer is the same as using their UserID and password.

e) Services available to the UserID should be consistent with the user's role and responsibilities within NHSGGC as agreed by the user's line manager. If any changes are made to the user's role, the relevant team should be notified & the account updated or removed.

f) Line Managers have a responsibility to ensure that their staff have read and comply with this policy.

g) The eHealth Department will ensure that all user network logins are configured to meet the minimum requirements.

h) If a user suspects that someone else may have become aware of his/her password the user must immediately change his/her password.

5.2.2 Maintenance of Personal Details

The personal details provided by you, location, role, line manager form part of your corporate digital persona. From that persona comes the creation of your UserID, email address and access to information, whether structured in a database or unstructured in a file share. If you use your NHS email address and password for an internet service and it becomes compromised then access to the NHS service can become compromised.

a) If your job role changes notify eHealth by updating your details on StaffNet so that your corporate digital persona can be updated.

b) To reduce the instances of compromise between corporate and personal life, subscription to non NHS services e.g. internet shopping, Social Media should be with a non-corporate persona e.g. personal email address, personal phone number etc.

c) When using NHS email for organisational purpose like corporate travel or professional body membership, users must ensure that they use a unique password.

d) Ensure that the user verification process maintained by the service desk has security questions and answers that only you will know, or two factor authentication. This improves response if you become locked out and reduce the risk of data breach.

5.3 Use of Authorised Equipment and Software

eHealth manages and updates authorised equipment and software. Unmanaged equipment or software brings risk to all equipment.

a) Do not connect unauthorised computer or networking equipment to the NHSGGC network, it may be insecure and a personal networking device can interrupt local network traffic preventing authorised devices from connecting.

b) Do not move static computer or networking equipment without authorisation. (Only in exceptional circumstances is it appropriate for non-eHealth staff to move or

connect equipment). Some computers, particularly medical equipment, will as part of their security posture be isolated and secured at the wall outlet. Reconnecting to another wall outlet, which may not be isolated can weaken the security of the device and the network.

c) As a member of staff leaves or their role changes then equipment should be returned to IT Asset Management or new user update provided.

d) Do not install unauthorised software on NHSGGC computer equipment. The software may not be secure and some software can be used to take control of the computer and provide an unauthorised route onto the NHSGGC network.

e) We need to ensure that a stolen computer can no longer access the network, our applications or data. If a computer is stolen, ensure that it is promptly reported through Datix or the IT Service Desk

f) Where non-NHSGGC owned equipment is to be connected to the NHSGGC network, this will be by agreeing security arrangements for that device with the IT Compliance Team. This can be discussed by raising a call with the IT Service Desk.

5.4 Email and Communication Activities

Email is the most prevalent digital communication mechanism within NHSGGC. As defined in the Email Acceptable Use Policy, our two approved email environments for NHS business use are GGC.SCOT.NHS.UK and NHS.Net. Mail can be sent securely to key partners within our secure email boundary without an additional security layer.

a) If staff wish to share access to their diary or emails then this must be done through delegated permissions, which is auditable.

b) Staff must not use personal email systems or include personal email addresses for any NHS business.

c) Staff must not use corporate email addresses (@GGC.scot.nhs.uk or @nhs.net) for personal use like internet shopping, social networking etc.

d) NHSGGC business, particularly the sending of Personal Identifiable Data, must only be carried out using @GGC.scot.nhs.uk or @nhs.net email address.

e) The sending of Personal Identifiable Data or otherwise sensitive data must follow the Email Acceptable Use Policy.

f) The only Personal Identifiable Data that can be sent to the IT Service Desk is the CHI number with no other accompanying identifiers.

5.5 Data Breach

Data Breaches can be intentional, where there has been a targeted approach to extract data from a system either by “hacking” or by social engineering where a member of staff is tricked into providing the data. Breaches can be unintentional, an email sent to the wrong address, providing more data than requested or data not appropriately

deleted. The breach may be discovered quickly or may take years. While data breaches have been significant under the Data Protection Act they acquire increased prominence through the General Data Protection Requirements. Investigation and reporting is defined in the NHS GGC Data Breach Policy.

a) All users of information systems need to conform with this policy

b) Each employee is personally responsible for ensuring that no breaches of computer security result from their actions.

c) If managers believe that there is a cause to initiate an investigation then they must contact a member of Human Resources. Please also refer to the NHSGGC Data Breach Policy.

d) If inappropriate use of any NHSGGC computer is suspected then investigations will be instigated under the direction of H.R. and may include Police or other regulatory body as appropriate. This will follow the NHSGGC Disciplinary Policy and Procedure.

5.6 Mobile Device Handling and Mobile Computing

Mobile computing devices, laptops, tablets and smartphones are now commonly used to access NHSGGC systems. The place of use has extended from NHS premises to partner organisations, patient home, your home or vehicle and public spaces. With these changes come additional security requirements.

a) To ensure protection from data loss, the mobile device must be encrypted or agreement reached with IT Compliance about the physical security measures that will be put in place to protect the device. This can be discussed by logging a call with the IT Service Desk.

b) To minimise service impact if the mobile device is lost or stolen it must not be the primary repository of that data. In order for data to be backed up the user must only save their documents in the “My Documents” folder (Documents folder for Windows 10) in order for them to get backed up when you connect to NHSGGC network.

c) Computers or media must not be left insecurely in public places or on open display in an unattended vehicle.

d) User must never directly connect to NHSGGC applications from insecure networks. Connection must be through an approved encrypted or virtual private network (VPN).

e) When in transit between places of work the device must be locked requiring use of username and password to unlock.

f) Confidential information must never be displayed in public areas.

g) Mobile devices must be connected to the NHSGGC internal network at least monthly in order to receive security updates (a wired connection is preferable because it will offer better performance and reliability).

h) LOSS or THEFT of any mobile device or removable media MUST:

- Be reported to the IT Service Desk
- Have a Datix incident submitted
- Be reported to the Police

(A reporting flow chart and responsibility diagram is included at Annex 8.1)

5.7 Internet Use

Use is defined in Internet Acceptable Use Policy. The Internet provides invaluable sources of information, learning and increasingly hosting of NHSGGC applications. Unfortunately accompanying the growth in legitimate Internet use has come malicious use so we need to adopt technology controls to protect our systems.

a) NHSGGC will monitor staff use of the Internet:

- To ensure that IT network performance meets business needs
- To protect the organisation from spyware, viruses, and malware
- To identify any inappropriate and excessive personal use
- To assure compliance with this policy

b) It is not appropriate for all internet sites to be accessed from the NHSGGC network. Controls are in place to prevent access to sites that NHSGGC and its security partners have categorised as inappropriate e.g. Fraudulent, harassing, illegal, embarrassing, sexually explicit, obscene, intimidating, racist, pornographic, defamatory or politically motivated. If users still encounter inappropriate material they should notify the IT Service Desk immediately.

c) Reasonable personal use of the Internet is permitted but only where it does not impact on business activities and is agreed by the line manager.

d) Care must be taken when opening web links, downloading and forwarding materials or sending links to web pages all of which can be malicious.

e) When material is downloaded, copied or reused then this must be in compliance with both the Copyright, Designs and Patents Act 1988, and the NHS Scotland Copy Policy 2011. Where is this

f) Internet use by UserID showing sites visited, time spent, downloads is captured in log files and is subject to inspection. Logs form one of the evidence sources if it is felt that this policy has been breached.

g) All staff have a requirement to inform their Line Manager immediately should they witness anyone accessing website material categorised broadly as:

- Images of child sexual abuse
- Criminally obscene content
- Incitement to racial hatred content

h) The Line Manager should, through the IT Help Desk or directly contact the IT Compliance Team with details of the user and site access. This will be used to support audit log preservation and prevent other inappropriate access.

i) Investigations of internet use would be progressed through request from HR.

5.8 Blogging and Social Media

Social media such as Facebook, YouTube, Twitter, Dropbox and instant messaging WhatsApp and Telegram will be widely used in personal life. There may be use cases where social media can be adopted for corporate use, like team communication but to ensure that it meets with Data Protection, Caldicott and corporate communications requirements, proposed use must be reviewed and agreed under the terms outlined in the following Policies; Personal Use Of Social Media and Corporate Use Of Social Media. Use of social media places significant responsibility on the service user to ensure appropriate us Treat what you post on social media as being in the public domain and not to be used for red/amber data.

j) The service user needs to ensure that their use of social networking and instant messaging meets with Data Protection, Caldicott and IT Compliance requirements.

j) These cannot be met using a personal social media account with personal identifiable data.

k) The service owner needs to understand the conditions of use of their provider.

l) Corporate use of social networking and instant messaging sites should only be considered after consultation with Corporate Communications and eHealth.

m) If using Social Media sites from home or from portable computers staff are reminded that they must continue to meet Data Protection and Caldicott requirements and may not refer to patients, staff members or any events that occur during work time on such sites. Please refer to the Policy on Personal Use of Social Media.

n) NHSGGC's Confidentiality and Data Protection Policy also applies to blogging. As such, employees are prohibited from revealing any NHSGGC confidential or proprietary information, trade secrets or any other material.

o) Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of NHSGGC and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct

prohibited by NHSGGC's Dignity At Work and Personal Use of Social Media Policies**.**

p) If you have a legitimate business reason to access these websites, please refer to the Corporate Use of Social Media Policy which can either be accessed from the link or by visiting the HRConnect.

q) Staff are not permitted to make unauthorised pictures, videos or audio recordings in healthcare settings that feature other service users, visitors or staff. No unauthorised pictures, videos or audio recordings, or comments identifying individuals, should ever be posted on any Social Media. Please refer to Pictures and Privacy on Social Media Policy.

5.9 Information Transfer

In line with the Data Protection Act, NHSGGC gathers data for a reason. There are partner organisations where there are established governance and technology protocols in existence for sharing information and there will be new requirements requiring new arrangements.

a) The first requirement is for users to confirm that there are formal confidentiality or non-disclosure agreements.

b) Once the agreement is in place the most appropriate secure data transfer mechanism can be agreed.

c) User must verify and then choose the correct and approved methods of transfer. In line with the Email Usage Policy, NHSGGC users can exchange sensitive information by email securely within NHSGGC and with other NHS users. They can also exchange with Partner Organisations or other secure Government organisations. This is the secure mail boundary for NHSGGC mail.

d) If users need to exchange information securely outside of the above secure email boundary then they need to use encryption. This is currently available within NHSmail by activating the NHSmail encryption feature. Encryption should primarily be used to exchange sensitive data as part of an agreed clinical workflow and should follow any local Information Governance policies that are in place for sending or receiving sensitive data.

e) Where data is being transferred on removable media then the media must be encrypted. The transfer must follow Media Handling Transfer Procedure. There will be a requirement to separately pass the decrypt key to the recipient.

f) Cloud services should only be used after consultation with eHealth. Most Cloud Services are not acceptable information transfer mechanisms for Patient Identifiable Data (PID) or any other sensitive data.

g) Media containing information must be protected against unauthorised access, misuse or corruption during transportation.

5.10 Use of Cloud Services

The most well-known cloud hosted file sharing services are Microsoft OneDrive, Google Drive, Dropbox and iCloud. Each service needs to have a defined owner who is responsible for managing access, content and compliance with Data Protection and Caldicott. Each cloud service provider will have their own security, backup and recovery models. Anyone wishing to use Cloud services needs to be clear about what their security and backup requirements are and what the exit conditions of their Cloud contract are. Some Cloud Services may have no charge, others will. Most have different terms and conditions between personal and corporate use. The service owner needs to establish what the use conditions are and where required, the payment mechanism.

a) Cloud services should only be used after consultation with eHealth.

b) Most Cloud Services are not acceptable information transfer mechanisms for Patient Identifiable Data (PID) or any other sensitive data.

6 Compliance with the Acceptable Use Policy

6.1 Compliance Measurement

NHSGGC will verify compliance to this policy via various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

6.2 Exceptions

Any exception to the policy must be by prior approval with the NHSGGC IT Compliance Team.

6.3 Non-Compliance

Breaching the policy may result in disciplinary action, up to and including termination of employment

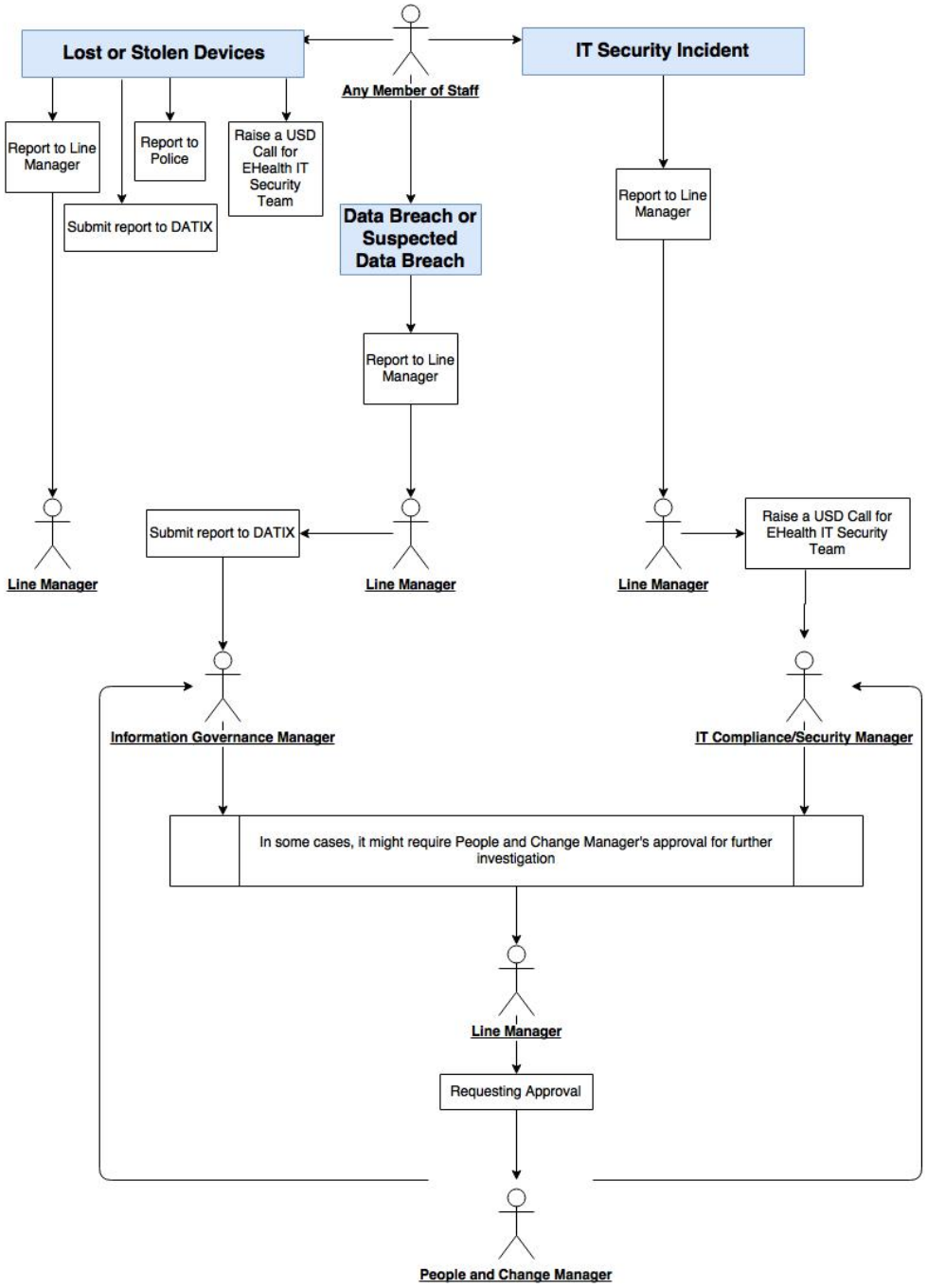
7 References

All relevant IT Security, Information Governance and other policies/procedures referred in this policy can be found in the below location in StaffNet IT Policies Page.

NHSGG&C Policy Title	Owner
Information Security Policy 1 Governance	IT Compliance
Information Security Policy 2 Risk Management	IT Compliance
Information Security Policy 3 Information Security	IT Compliance
Information Security Policy 4 ISMS	IT Compliance
Information Security Policy 5 Organisation	IT Compliance
Information Security Policy 6 Human Resource	IT Compliance
Information Security Policy 7 Asset Management	IT Compliance
Information Security Policy 8 Access Control	IT Compliance
Information Security Policy 9 Cryptographic	IT Compliance
Information Security Policy 10 Physical and Environmental	IT Compliance
Information Security Policy 11 Operations Security	IT Compliance
Information Security Policy 12 Communications	IT Compliance
Information Security Policy 13 Data Transfer	IT Compliance
Information Security Policy 14 System Acquisition	IT Compliance
Information Security Policy 15 Supplier Relationships	IT Compliance
Information Security Policy 16 Incident Management	IT Compliance
Information Security Policy 17 Business Continuity	IT Compliance
Information Security Policy 18 Compliance	IT Compliance
Personal Use of Social Media	Human Resources
Corporate Use of Social Media	Human Resources
Dignity at Work	Human Resources
Disciplinary Policy and Procedure	Human Resources
Confidentiality & Data Protection Policy	Information Governance
Clear Desk Policy	Information Governance
Pictures and Privacy on Social Media	Information Governance
Data Breach Policy	Information Governance
NHS Scotland Copy Policy	Library Services
Communicating with the NHS Scotland IT Service Desk	External : NHS Scotland
Copyright, Design and Patents Act 1988	External : Legislation
NHS Scotland Information Security Policy Framework (2018)	Scottish Health Competent Authority

8 Annexes

8.1 Escalation/Reporting Flow for any IT Security or Data Breach Incidents



8.2 AUP Topic Relationship to Other Policies

All relevant IT Security, Information Governance and other policies/procedures referred in this policy can be found in the below location in StaffNet IT Policies Page.

AUP Topics	IT Security Framework Policies	Non IT Security Framework Policies/Procedures
General Use of Information Systems	• Governance • Risk Management • ISMS • Organisation • Human Resources • Compliance • Access Control • Information Security Policy • Organisation of Information Security : Mobile Devices and Teleworking	• Confidentiality & Data Protection Policy • Network Account Deletion Policy • Disciplinary Policy and Procedure • Data Breach Policy • Password Policy
Identity and Access Management and keeping personal details up to date	• Governance • Risk Management • ISMS • Organisation • Human Resources • Access Control • Information Security Policy • Supplier Relationships	• Confidentiality & Data Protection Policy • Network Account Deletion Policy • Disciplinary Policy and Procedure • Data Breach Policy • Password Policy • Administrator Accounts
Use of Authorised Equipment and Software	• Governance • Risk Management • ISMS • Organisation • Data Transfer • Compliance • Operations Security • Access Control • System Acquisition • Physical and Environmental • Asset Management	• Confidentiality & Data Protection Policy
Email and Communication Activities	• Governance • Risk Management • ISMS • Organisation • Data Transfer • Cryptographic Control • Access Control	• Email Usage Policy • NHSmail Acceptable Use Policy • Password Policy
Data Breach	• Governance • Risk Management • ISMS • Organisation	• Data Breach Policy

	• Human Resources • Compliance • Access Control • Information Security Policy • Incident Management	
Mobile Device Handling and Mobile Computing	• Governance • Risk Management • ISMS • Organisation • Data Transfer	• Password Policy • Organisation of Information Security : Mobile Devices and Teleworking
Internet Use	• Governance • Risk Management • ISMS • Organisation • Data Transfer • Access Control	• Internet Acceptable Use Policy • NHS Scotland Copy Policy 2011 • Copyright, Designs and Patents Act 1988 • Password Policy
Blogging and Social Media	• Governance • Risk Management • ISMS • Organisation • Data Transfer • Access Control	• Internet Acceptable Use Policy • Personal Use Of Social Media • Corporate Use Of Social Media • Confidentiality And Data Protection Policy • Dignity At Work • Pictures And Privacy On Social Media • Password Policy
Information Transfer	• Governance • Risk Management • ISMS • Organisation • Data Transfer • Cryptographic Control	• Email Usage Policy • Media Handling Transfer Procedure • Password Policy
Use of Cloud Services	• Governance • Risk Management • ISMS • Organisation • Data Transfer • Access Control	• Internet Acceptable Use Policy • Password Policy

8.3 Learning Material

Subject	Provider/Link
Be Cyber Safe	http://www.staffnet.ggc.scot.nhs.uk/Corporate%20Services/eHealth/BCS/Pages/CyberSecurity.aspx
Basic Computing Skills training session	NHSGGC Library Services http://www.staffnet.ggc.scot.nhs.uk/Corporate%20Services/eHealth/LN/Pages/BasicIT.aspx

Basics of Using the Internet	http://www.staffnet.ggc.scot.nhs.uk/Corporate%20Services/eHealth/LN/Pages/BasicIT.aspx
NHS Elite is a learning and assessment tool covering the essential IT skills that are required for most NHS Staff	https://nhs.learnprouk.com
Safe Information Handling	https://nhs.learnprouk.com
Information Handling in Practice	https://nhs.learnprouk.com
Security	https://nhs.learnprouk.com
IT systems and applications at NHS Greater Glasgow and Clyde: A guide for Acute Services	http://www.staffnet.ggc.scot.nhs.uk/Corporate%20Services/Health%20Information%20Technology/AApp/Documents/!General%20docs/A%20guide%20for%20New%20Medical%20Staff.pdf
Safe Internet Browsing Cyber Crime Social Media and Internet Dating Phishing and Internet Shopping	Police Scotland http://www.scotland.police.uk/keep-safe/keep-secure-online/
Social Engineering Stop that Phish Top Tips to securely using Social Media Securing Your Mobile Devices Email Do's and Don'ts	SANS Institute Newsletters OUCH https://www.sans.org/security-awareness-training/ouch-newsletter