NHS
Greater Manchester Shared Services

GMSS Acceptable Use of IT / Information Systems Policy – (Tier 1)

Review Date: November 2021

Document Control

Title / Reference:	Acceptable Use of IT / Information Systems Policy (ISMS-C_DOC_8.1.3)
Status:	Approved
Version:	V3.2
Date Issued / Ratified:	Jan 2020
Originator of Document and Job Role:	IG Team and Phil Scott – IT Security Manager
File Classification:	Official Data
Retention:	Life of the organisation plus 6 years (place of deposit)
Target Audience:	All GMSS staff & 3rd party partners
Links to other strategies, policies, procedures etc:	• ISMS Manuel • Data Security & Protection (IG) Framework • Data Security Protection & Confidentiality Policy • Information Security Policy **This list is not exhaustive**

Change History

Summary of Changes	Name	Date	Version
Amendments and reviewed from Oldham CCG to fit GMSS	IG Team	Nov 16	1.0
Recommend approval by the IG Group	IG Group	Nov 16	1.0
Recommend approval after some amendments	FPG	Jan 17	1.0
Amendments needed	SMT	Jan 17	1.0
S8.23 amended to allow for the use of Skype	Head of IG	May 17	2.0
Changed formatting to bring in line with ISO27001 documents. Added section 1 'Scope' added S8.27, S8.28, S8.29, S8.30,S8.31 to define e-mail usage	Phil Scott	05/08/19	3.0
Amendments made in line with NHS Digital Guidelines	Caroline Cross	07/08/19	3.1
Added Telephone acceptable use section	Phil Scott	17/09/19	3.2
Amendments made per Governance Committee review (use consistent GMSS template)	IG Team	11/12/19	3.2

Review

Name	Role	Date	Version
Governance Committee	Governance Committee members	Nov 19	3.2

Approval

Name	Role	Date	Version
IG Group	IG Group	Nov 19	3.1
Governance Committee	Governance Committee	Dec 19	3.2
SMT	SMT	Jan 20	3.2

Distribution

Name	Role	Date	Version
Saved in policy folder		Nov 19	3.2
Updated policy tracker		Nov 19	3.2
GMSS Publication scheme		Feb 20	3.2
The Bulletin		Feb 20	3.2
People Matters		Feb 20	3.2

DOCUMENT STATUS:
This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of the document are not controlled

Contents

1. Scope

All employees and authorised third parties that access GMSS managed IT and Information services are in scope of this policy.

2. Assurance Statement

This Policy describes the responsibilities and acceptable use of IT and Information assets within Greater Manchester Shared Services (henceforth referred to as GMSS). This policy is adopted from NHS Digital Guidance.

GMSS reserves the right to amend this policy without notice. If any changes to this policy affect the way employees' use the IT services and information assets, GMSS will provide an avenue for this information to be cascaded down to members of staff and provide reasonable time for the change to be implemented. Employees are responsible for reviewing the policy from time to time.

All staff will be required to have sight of this policy and be appropriately authorised by their manager prior to gaining access to the IT network. All updates to the policy will be communicated to staff by briefings and the Intranet.

3. Introduction

This policy covers the following areas for acceptable use:

- Use of Information Systems:
    - Unauthorised Information Access
    - Misuse of Information Systems

- Guidelines for IT Equipment Use:
    - Physical Protection
    - General Use
    - Internet Acceptable Use
    - NHS Mail Acceptable Use
    - Telephone Acceptable Use

- Duties & Responsibilities;
- Monitoring Arrangements;
- Equal Analysis.

Any applications, e.g. NHS mail, will also be subject to the NHS terms and conditions of use and their acceptable use policy.

4. Aims and Objectives

This policy applies to those members of staff that are directly employed by GMSS and for whom GMSS has legal responsibility including Agency and Interim staff. For those staff covered by a letter of authority/honorary contract or work experience the organisation's policies are also applicable whilst undertaking duties for or on behalf of GMSS. Further, this policy applies to all third parties and others authorised to undertake work on behalf of GMSS.

For the purposes of this policy the aforementioned will be referred to as users throughout the remainder of this document.

5. Use of IT / Information Systems

Unautorised Information Access:

- GMSS and third-party employees shall only be authorised access to IT systems and information relevant to their work.
- Accessing or attempting to gain access to unauthorised IT systems and information shall be deemed a disciplinary offence.
- When access to IT systems and information is authorised, the individual user shall ensure the confidentiality and integrity of the IT systems, and information is upheld, and to observe adequate protection according to NHS policies as well as legal and statutory requirements. This includes the protection of IT systems and information against access by unauthorised persons.

All staff must be made aware that they have a duty of care to prevent and report any unauthorised access to systems, information and data.

Misuse of IT Systems:

Use of NHS IT systems for malicious purposes shall be deemed a disciplinary offence. This includes but is not limited to:

- Penetration attempts ("hacking" or "cracking") of external or internal systems.
- Unauthorised electronic eavesdropping on or surveillance of internal or external network traffic.
- Discriminatory (on the grounds of sex, political, religious or sexual preferences or orientation), or derogatory remarks or material on computer or communications media; this includes but is not limited to sending offending material as embedded or attached information in e-mails or other electronic communication systems.
- Acquisition or proliferation of pornographic or material identified as offensive or criminal.
- Deliberate copyright or intellectual property rights violations, including use of obviously copyright-violated software.
- Storage or transmission of large data volumes for personal use, e.g. personal digital images, music or video files or large bulk downloads or uploads.
- Users accessing or attempting to access medical or confidential information concerning themselves, family, friends or any other person without a legitimate purpose and prior authorisation from senior management is strictly forbidden and shall be deemed a disciplinary offence.

Use of NHS IT and information systems or data contained therein for personal gain, to obtain personal advantage or for profit is not permitted and **shall** be deemed a disciplinary offence.

If identified misuse is considered a criminal offence, criminal charges shall be filed with local police and all information regarding the criminal actions handed over to the relevant authorities.

All staff must be made aware of what constitutes misuse and the potential consequences of any misuse of systems, information and data.

6. Guidelines for IT Equipment Use

Physical Protection

- Users shall not expose any IT equipment to magnetic fields which may compromise or prevent normal operation.
- Users shall not expose any IT equipment to external stress, sudden impacts, excessive force or humidity.
- Only authorised IT support personnel shall be allowed to open NHS IT equipment and equipment cabinets.
- Portable equipment shall never be left unattended in un-controlled areas such as airport lounges, hotel lobbies and similar areas as these areas are insecure.
- Portable equipment shall be physically locked down or locked away when left in the office overnight.
- Portable equipment shall never be left in parked cars, unless completely invisible from outside the vehicle and protected from extreme temperatures. Devices must not be left in any vehicle overnight.
- Portable equipment shall not be checked in as hold luggage when travelling, but treated as hand or cabin luggage at all times.

General Use

- Users shall lock their terminal/workstation/laptop/mobile device (using the Ctrl-Alt-Delete function or other applicable method) when left unattended, even for a short period.
- Users shall not install unapproved or privately owned software on NHS IT equipment.
- Users shall not tamper with, attempt to uninstall, reimage or factory reset any NHS IT equipment.
- Only authorised GMSS IT personnel shall be allowed to reconfigure or change system settings on the IT equipment.

Laptops and mobile devices shall:

- Only be used by the NHS or third party employee that has signed and taken personal responsibility for the laptop.
- Have the corporate standard encryption software installed, rendering the information on the laptop inaccessible if the laptop is stolen or lost.
- Have the corporate standard anti-virus, anti-spyware and personal firewall software installed.
- Have the corporate standard remote access installed.

If configured according to the specifications above the laptop/mobile device may be connected to wired or wireless access points.

- NHS laptops shall never be (via cable or wireless) directly connected to other non-NHS IT equipment or systems.
- Users shall not use privately owned storage devices or storage devices owned by third parties for transfers of NHS data.
- Any device lost or stolen shall be reported immediately to the GMSS IT Security Team.
- Users shall accept that personal use of the GMSS information systems is not a right and must be exercised with discretion and moderation. Users further accept GMSS will not accept any liability, in part of whole, for any liability for

claims arising out of personal use of the GMSS information systems or GMSS information.

The GMSS retains the right to:

- Request the monitoring of the use of its IT and information systems for the purpose of protecting legitimate concerns, prohibit personal use of IT and information systems without warning or consultation whether collectively, where evidence points to a risk to GMSS and / or constituent businesses, or individually where evidence points to a breach of this or any pther GMSS or NHS policy.
- In addition, such devices must be transported securely and may only be left in the boot of a car during the day when there is no alternative method of securing the device. Devices must not be left in any vehicle overnight.

Users are not permitted to share their, or others, usernames or passwords to gain access to any GMSS or other IT and information systems.

Users **shall** follow established procedures for password changes and are not permitted to disclose or write down their passwords.

Telephone Acceptable Use

- The GMSS telephones are provided for business use in order to assist staff in carrying out official business.
- It is accepted that there are occasions when making personal calls at work cannot be avoided. However, it should be remembered that calls are logged and abuse of a telephone system or mobile telephone may result in disciplinary action.
- Such monitoring of telephone use will comply with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the Data Protection Act 2018. It will be used to establish facts, confirm legitimate business use and compliance with this Policy.
- Mobile phone users are required to read, understand and adhere to the GMSS Mobile Phone Acceptable Use Policy.

Internet Acceptable Use

- Information found on the Internet is subject to minimal regulation and as such must be treated as being of questionable quality. You should not base any business-critical decisions on information from the Internet that has not been independently verified.
- Internet access via the NHS infrastructure is provided for business purposes. For the purpose of simplifying everyday tasks, limited private use may be accepted.
- Excessive personal use of the Internet during working hours shall not be tolerated and may lead to disciplinary action. Any personal use should be in own i.e. lunch break time and will not count as part of working hours.
- Users shall not use Internet-based file sharing applications, unless explicitly approved and provided as a service.
- Users shall not upload and download private data (e.g. private pictures) to and from the Internet.
- Users shall not download copyrighted material such as software, text, images, music and video from the Internet.

- Users shall not use NHS systems or Internet access for personal advantages such as business financial transactions or private business activities.
- Users shall not use their GMSS identity (i.e. using your NHSmail e-mail address) for private purposes such as on social media, discussion forums.

NHS Email Acceptable Use

- Email services within the NHS are provided for business purposes. Limited private use for the purpose of simplifying everyday tasks may be accepted but private emails should be distributed via web based email services and not using NHS Mail.
- Users shall not use external, web-based e-mail services (e.g. hotmail.com) for business communications and purposes.
- Any private emails should be stored in a separate folder named 'Private e-mail box'. If retrieval of business emails is required (due to sick leave etc.) this folder will not be subject to inspection).
- Any private emails should be deleted as soon as possible in order to limit storage requirements for non-business information.
- Users shall not broadcast personal messages, advertisements or other non-business related information via NHS e-mail systems.
- Users shall not distribute content that might be considered discriminatory, offensive, derogatory, abusive, indecent, pornographic or obscene.
- Users shall not distribute statements of a political or religious nature, or other information of a personal nature.
- Engaging in any illegal activities via e-mail is prohibited. Discovery of such material shall, if deemed as being of a criminal nature, be handed over to the police.

7. Duties and Responsibilities

Overall responsibility for the Acceptable Use policy lies with the Managing Director who has delegated responsibility for managing the development and implementation of procedural documents to the IT Service Provider and line managers.

The GMSS Information Governance Team will provide IG advice and guidance in line with contractual obligations and support GMSS management where applicable.

Staff will receive instruction and direction regarding the policy from a number of sources:

- Policy and Strategy Manuals
- Line Manager
- Specific training course
- Other communication method (e.g. team briefing and intranet)

Staff must be aware that it may be a disciplinary offence to make disparaging or libellous remarks about their employer, patients or other employees even when using their own computer at home on social networking sites.

GMSS requires all employees to be treated with dignity at work, free from harassment and bullying of any kind. Harassment can take the form of general bullying, or be on the grounds of sex, transgender, non-binary, race, disability, sexual orientation, age, religion and pregnancy/maternity. Harassment could include sending sexist or racist comments or behaviour, making sexual propositions or general abuse by e-mail. You

must not send any messages containing such material. Bullying and harassment of any kind will be treated as a serious disciplinary matter which may lead to dismissal. If you are subjected to or know about any harassment or bullying, whether it comes from inside or outside the organisation you are encouraged to contact your line manager/HR advisor immediately.

8. Training and Awareness

This policy will be made available to all staff via The Bulletin and published on GMSS Website and on People Matters for GMSS staff.

All staff are responsible for adhering to the General Data Protection Regulations 2016, Caldicott Principles, the National Data Guardian Data Security Standards, the Data Protection Act 2018 and the common law duty of confidentiality.

All staff are mandated to undertake Data Security Awareness training on an annual basis.

Staff will receive guidance regarding this policy from a number of sources:

- Policies and procedure located on People Matters;
- Line manager;
- Other communication methods (e.g. staff briefings, team meetings, IG updates).
- The IG Team and/or IT Security Manager.
- Other training methods will be used as necessary to meet individual needs due to disability.

9. Classification of Information

GMSS implement appropriate information classifications controls, based upon the data security legislation.

Further details of the classifications controls can be found in the Information Classification Policy and the Records Management Policy.

10. Legislation & Guidelines

A set of procedural documents will be made available via People Matters.

- General Data Protection Regulations 2016
- Data Protection Act 2018
- The National Data Guardian Data Security Standards
- Confidentiality: NHS Code of Practice
- Common Law Duty of Confidence
- Human Rights Act 1998
- Computer Misuse 1998
- Electronic Communications Act 2000
- Guide to the Notification of Data Security and Protection Incidents.

11. Equality Statement

GMSS aims to design and implement services, policies and measures that are fair and equitable. As part of its development, this policy and its impact on staff, patients and

the public have been reviewed in line with the GMSS legal equality duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, patients and the public on the grounds of race, socially excluded groups, gender, transgender, non-binary, disability, age, sexual orientation, pregnancy/maternity or religion/belief.

The Equality Analysis has been completed and any associated policies and procedures will be analysed accordingly.

12. Monitoring and Review

This policy will be monitored through staff awareness and supporting evidence to the Data Security & Protection Toolkit.

This policy will be reviewed on a two yearly basis and in accordance with the following as and when required:

- Legislative changes;
- Good practice guidance;
- Case law;
- Significant incidents reported;
- New vulnerabilities; and
- Changes to organisational infrastructure.

The next review is scheduled for November 2021.