Greater Manchester Shared Services

GMSS

Acceptable Use Policy

Review Date: October 2019

Programme:	Greater Manchester Shared Services
Filename:	I:GMSS/IG Policies & Procedures/ Updated GMSS Policy
Author:	IG Team
Version:	2.0
Date Released:	October 2017
Purpose of this document:	This document outlines GMSS Acceptable Use of IT Policy

Document Location

Copies of this document can be obtained from|:

Name:	Corporate Services Office
Address:	Greater Manchester Shared Services Ellen House Waddington Street Oldham OL9 6EE
Telephone:	0161 212 4186

Revision History

Revision date	Revision by	Summary of changes	Version
Nov 2016	IG Team	Amendments and reviewed from Oldham CCG to fit GMSS	1.0
Nov 2016	IG Group	Recommend approval by the IG Group	1.0
Jan 2017	FPG	Recommend approval after some amendments	1.0
Jan 2017	SMT	Amendments needed	1.0
May 2017	Head of IG	S7.23 amended to allow for the use of Skype	2.0
Sept 2017	IG Team	Reviewed to accommodate GDPR	2.1
October 2017	Head of IT	Comments Received	2.1

Approvals

Name	Role	Date	Version
K Rigden	Approval and gave assurance	Jan 2017	1.0
SMT	Amendment of S7.23 Approved by SMT	9th May 2017	2.0
IT		20th May 2017	2.1

Distribution

Name	Role	Date	Version
Saved in policy folder		June 2017	2.1
Updated Policy Tracker		December 2017	2.1
GMSS Publication		December 2017	2.1

scheme			
Shared in the Bulletin		December 2017	2.1

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. Assurance Statement

1.1 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 the NHS England Policy of the same name.

1.2 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.

1.3 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.

2. Introduction

2.1 This policy covers the following areas for acceptable use:

- Responsibilities and use of IT assets
- Use of email and internet
- Network usage

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

3. Aims & Objectives

3.1 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.

3.2 For the purposes of this policy the aforementioned will be referred to as users through the remainder of this document

4. Prohibited Use

4.1. Use of the internet for the following is strictly forbidden at any time, and anyone using the Internet inappropriately may be disciplined and/or prosecuted

- Pornography (e.g. accessing child pornography is illegal)
- Illegal or commercial activities (e.g. sites promoting violence, racial discrimination or sexual harassment, sites that are defamatory or that are intended to harass or intimidate other staff or using NHS resources to operate a business from work or advertising)
- Activities for financial gain (e.g. lotteries, gambling)
- Downloading material protected by copyright unless express permission has been given (Copyright Designs and Patents Act 1988)
- Hacking (e.g. breaking into other computer systems using the NHSR network as a conduit)
- Fraud (e.g. providing false details or attempting to gain profit illegally

If you have any questions about what is considered to be appropriate or inappropriate use, please check with your manager or the IT Department. Known sites falling within the above categories may be blocked by web security software.

If you require access to a site that is being blocked by the web security software, contact GMSS IT Service Desk in the first instance on 0161 765 6685.

5. Definition of Terms

5.1 Information Asset

Information assets are definable information resources owned or contracted by an organisation that are 'valuable' to the business of the organisation.

5.2 Malware

Software intended to cause harm or disruption to computers or networks. There are many classifications of Malware (malicious software) but as a general term it deals with all forms of viruses, spyware, Trojans and other software designed with malicious intent.

5.3 Spam

Mass unsolicited electronic mail received from an un-requested source which attempts to convince the user to purchase goods or services. SPAM consumes valuable network resources while delivering no business benefit.

5.4 Blogging or Tweeting

This is using a public website to write an on-line diary (known as a blog) or sharing thoughts and opinions on various subjects. Blogs and Tweets are usually maintained by an individual with regular entries of commentary, descriptions of events, and may include other material such as graphics or video Examples of blogging websites include Twitter.com and Blogging.com.

5.5 Social Media

This is the term commonly used for web-based and other mobile communications technologies that enable messages and opinions to be shared in dialogue with others.

5.6 Social Networking

This is the use of interactive web based sites or social media sites, allowing individuals on-line interactions that mimic some of the interactions between people with similar interests that occur in life. Popular examples include Facebook.com and Linkedin.com

5.7 Social Engineering or Blagging

This is the method whereby an attacker uses human interaction (social skills) to deceive others to obtain information about an organisation and its information assets including personal data. An attacker may potentially masquerade as a respectable and plausible person claiming bona fide interest in the information concerned e.g. posing as a member of the organisation's staff or maintenance contractor etc.

5.8 Intellectual Property Breach

Data / information is a valuable commodity, and much like any other market economy, principles of supply and demand drive it. As risks increase and profits decline,

cyber criminals are on the rise. Intellectual Property breach can include unauthorised access, copying or disclosure of a research protected by trade mark, copyrighted materials, and other such information.

6. Duties and Responsibilities

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

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

6.3 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).

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

6.5 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, race, disability, sexual orientation, age, religion. Harassment could include sending sexist or racist jokes, 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.

7. Main Policy

7.1 All data and information relating to GMSS residing on GMSS information system remains the property of GMSS at all times, unless otherwise stated.

7.2 Users accept that personal use of 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 GMSS information systems or GMSS information.

7.3 GMSS retains the right to:

- Request the monitoring of the use of its information systems for the purpose of protecting legitimate concerns
- prohibit personal use of information systems with 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 other GMSS or NHS policy.

7.4 Users are not permitted to access, attempt to access, circumvent, attempt or cause to circumvent, established security mechanisms or controls to view, modify, delete or transmit information and/or information systems to which they have not given explicit access or authorisation.

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

7.6 Users are not permitted to access any information to which they have not been given explicit authorised access.

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

7.8 Users are strictly prohibited from installing software on GMSS or other NHS supplied device.

7.9 It is mandatory for all users to lock their terminals, workstations, laptops, by pressing ctrl/alt/del (or "windows key" and L), iPads and/or Smartphones when not using the device, even for a short period.

7.10 Authorised staff and IT users will be permitted to use their personal devices to connect to a GMSS network, but will not be permitted to connect to GMSS corporate domain. In doing so, they must abide by all policies, standards, processes and procedures.

7.11 Illegal downloads, copying and/or storage of copyrighted content onto GMSS information systems is strictly prohibited.

7.12 All users must follow Health and Safety guidelines when using information systems.

7.13 Users will adhere to Management guidelines, the Information Classification document and information encryption policy when sharing, or sending GMSS information internally or externally.

7.14 Users are strictly prohibited from using GMSS information systems and information in a manner that will:

- Break the law and / or have legal implications or liability to GMSS and/or constituent business
- cause damage or disruption to GMSS information systems, including that its constitute businesses
- violate any provision set out in this or any other policy, or contravene GMSS Code of Conduct/Standards of Business Conduct and waste time, decrease productivity or prevent the user from performing their primary responsibilities for GMSS

7.15 Usage of GMSS Internet is primarily for business use. Occasional and reasonable personal use is permitted, e.g. during breaks, provided that such use does not interfere with performance of duties and does not conflict with GMSS policies, procedure and contracts of employment.

7.16 Users must, at all times, comply with Copyright, Design and Patent Laws, when downloading material from Internet sites.

7.17 GMSS prohibits access to websites deemed inappropriate and monitors access and usage. The monitoring information may be used to support disciplinary action.

7.18 Sites deemed inappropriate are those with material that is defamatory, pornographic, sexist, racist, on-line gambling, terrorism and/or such sites whose publication is illegal or risks causing offence.

7.19 Users must not circumvent, cause to circumvent or use tools to circumvent prohibited website controls. If a user inadvertently accesses an inappropriate website, the user must immediately inform their line manager or the IT Service Desk.

7.20 Financial transactions are not permitted on websites requiring software to be downloaded prior to the transaction being executed. GMSS accepts no responsibility for any charges and/or losses incurred in relation to personal purchases or personal transactions using GMSS information systems regardless of cause. Users are prohibited from having personal items delivered to GMSS premises.

7.21 The use of GMSS information systems to conduct on-line selling is strictly prohibited.

7.22 Only GMSS approved standard and supported Instant Messaging software may be used for business purposes. Users are prohibited from using any other software, not approved by GMSS, for Instant Messaging. Users must not circumvent, cause to circumvent, or use tools to circumvent established security and controls applied to any GMSS Instant Messaging or other communications software

7.23 Only approved software systems for video conferencing and collaborative working must be used. The systems must be used in accordance with NHS guidance

7.24 Those staff issued with mobile computing devices including, but not limited to, tablet PCs, laptops, netbooks, smart phones etc., must ensure that the equipment is secure at all times.

7.25 Equipment will not be left on office desks over night; they must be locked securely away. 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.

7.26 Users of mobile computing devices will not allow unauthorised access by third parties including, but not limited to, family and friends.

8. Monitoring Arrangements

8.1 Monitoring the Policy

Users of the Internet must be aware that each site they visit is recorded and logs of sites may be examined to ensure inappropriate usage is dealt with. A full security audit trail may be maintained of records/sites accessed.

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

- legislative changes
- good practice guidance
- case law
- significant incidents reported
- new vulnerabilities
- organisational changes

8.3 **Equality Analysis**

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 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, disability, age, sexual orientation or religion/belief.

The Equality Analysis has been completed and has identified impact or potential impact as "no impact"

9. Legislation & Other Related Documents

This policy and a set of procedural document manuals are available in GMSS folders.

Related policies are below that all employees should be aware::

- Information Security Policy