NHS
Greater Manchester Shared Services

GMSS Information Classification Policy - (Tier 2)

Review Date: November 2021

Document Control

Title / Reference:	Information Classification Policy (ISMS-C_DOC_8.2)
Status:	Approved
Version:	V1.0
Date Issued / Ratified:	Jan 2020
Originator of Document and Job Role:	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 Manual • Records Management Policy

Change History

Summary of Changes	Name	Date	Version
New Document	Phil Scott	24/07/19	0.1
Amended classification labelling requirements	Phil Scott	23/10/19	0.2
Amendments made per IG Group	IG Team	24/11/19	0.3
Amendments made per Governance Committee review (use consistent GMSS template)	IG Team	11/12/19	0.4

Review

Name	Role	Date	Version
IG Group	IG Group	Oct 19	0.2
Governance Committee	Governance Committee	Nov 19	0.4
Senior Management Team	Senior Management Team	Jan 20	1.0

Approval

Name	Role	Date	Version
IG Group	IG Group	Oct 19	0.2
Governance Committee	Governance Committee	Nov 19	0.4
Senior Management Team	Senior Management Team	Jan 20	1.0

Distribution

Name	Role	Date	Version
Saved in policy folder		Nov 19	1.0
Updated policy tracker		Nov 19	1.0
GMSS Publication scheme		Feb 20	1.0

The Bulletin		Feb 20	1.0
People Matters			

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. Purpose 5
2. Scope 5
3. Responsibilities 5
4. Classification 5
5. Classification Labels 6
6. Classification Labelling 6
7. Handling 6
8. Training and Awareness 7
9. Classification of Information 7
10. Legislation & Guidelines 7
11. Equality Statement 7
12. Monitoring and Review 8

1. Purpose

The purpose of this Information Classification Policy is to provide guidance in line with HMG Cabinet Office direction for the implementation of an organisation wide Information Classification Policy.

This is in order to ensure that the applicable and relevant security controls are set in place in line with the Department of Health and Social Care, the wider NHS, health and social care and HMG requirements.

2. Scope

All Greater Manchester Shared Services information assets and services (see control section 8.2 of the ISO27001 ISMS Manual) are classified, taking into account their legality, value, sensitivity and criticality to GMSS.

3. Responsibilities

The owner of each asset (see control section 8.1.2 of the Manual) is responsible for its classification, for ensuring it is correctly labelled and for its correct handling in line with its classification.

The Head of IT is responsible for the technical labelling mechanisms.

Line managers/ Information asset owners are responsible for ensuring that mail/postal services (work instruction **ISMS-C DOC 8.1.3c**), voicemail and voice communication (work instruction **ISMS-C DOC 8.1.3d**), fax machines (work instruction **ISMS-C DOC 8.1.3e**), photocopiers (**ISMS-C DOC 8.1.3f**), couriers, [other services], and sensitive documents (including cheques, invoices, headed notepaper) are handled in line with specific work instructions.

All staff must follow the Classification User Procedure which sits alongside this policy.

4. Classification

Greater Manchester Shared Services classifies information into three levels of classification (Patient identifiable data and personal data, Official data and public data).

The classification level of all assets is identified, both on the asset (see control section 8.2.2 of the Manual) and in the asset inventory (see control section 8.1.1 of the Manual).

The classification information must be included within the document, which must be set to appear on the front page of the document, or on the media on which it is recorded, in line with Clause 8, below.

Information received from outside Greater Manchester Shared Services is re-classified by its recipient (who becomes its *owner*) so that, within Greater Manchester Shared Services, it complies with this procedure.

Information that is not marked with a classification level is returned to its sender for classification; if it cannot be returned, it is destroyed.

The classifications of information assets are reviewed every six months by their

owners and if the classification level can be reduced, it will be. The asset owner is responsible for de-classifying information.

5. Classification Labels

Patient Identifiable Data and Personal Data

This classification applies to information that contains medical records or personal data i.e. patient letters, HR information, home contact information etc.

Information classified as Patient identifiable data and personal data sent by e-mail must be encrypted, in line with the control section 10.1 of the Manual, and sent only to the e-mail box of the identified recipient.

Official Data

The Official Data classification applies to information that routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened risk profile. E.g. Contractual documentation, audit reports, operational documentation/procedures, project admin data.

Information classified as Official data sent by e-mail must be encrypted, in line with the control section 10.1 of the Manual, and sent only to the e-mail box of the identified recipient.

Public Data

This classification applies to information if it is released to public domains; E.g. website content, public communications, approved media releases, published research etc.

6. Classification Labelling

Documents are labelled as set out above, on the front page of the document.

Electronic documents and information assets are labelled by the user when creating a new document as per the classification procedure.

All e-mails have a standard disclaimer at the foot of each email to the effect that the views expressed in the e-mail are those of the sender alone and do not reflect the views of Greater Manchester Shared Services.

7. Handling

Information assets can only be handled by individuals that have appropriate authorisations.

The requirements for transmission, receipt, storage and declassification of classified and restricted information are described above. Destruction of information media can only be carried out by someone who has an appropriate level of authorisation and in line with the requirements of ISMS-C DOC 8.3

Portable and storage media (including spooled media) must be moved, received and stored on the basis of the highest classification item recorded on them, and are subject to the physical security controls specified in ISMS-C DOC 11.2.1, and are encrypted

while being recorded.

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 and/or IT Security updates).
- The IG Team and/ or IT Security Manager.

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, disability, age, sexual orientation 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.