Greater Manchester Shared Services

GMSS Information Governance & Cyber Security Incident Reporting Policy

Review date: October 2019

Programme:	Greater Manchester Shared Services
Filename:	I:\GMSS\GDPR\POLICIES
Author:	GMSS IG Team
Version:	1.2
Date Released:	October 2017
Purpose of this document:	This document outlines GMSS Information Governance & Cyber Security Incident Reporting 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
20 April 2015	SC	First draft	D1.0
28 April 2015	SC	Changes made in line with new guidance from NHS England	D2.0
27 July 2015	GC	Final updates by head of Integrated Governance to maintain relevance to GM staff	D3.0
19 Feb 2017	GC	Head of IG review and IT security manager review – update for FGP approval	D4.0
August 2017	GMSS IG Team	Changes to accommodate GDPR	1.1

Approvals

Name	Role	Date	Version
Director		February 2016	V1.0
SMT		28 Feb 2017	V1.0
IG		18th October 2017	V1.2

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

INFORMATION GOVERNANCE & CYBER SECURITY INCIDENT REPORTING POLICY

1.0 Introduction

1.1 Due to the increase in Information Governance and Cyber Security incidents, NHS DIGITAL have introduced documentation called the "Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation" and on-line reporting via the IG Toolkit. The guidance covers reporting arrangements and actions that need to be taken when an IG / cyber security incident and / or IG Serious Incident Requiring Investigation (SIRI) occurs. It also contains guidance regarding scoring an incident based on numbers of individuals affected together with other sensitivity factors. It is important as it defines when an incident becomes an IG SIRI. For a reported IG incident to become an IG SIRI, a level 2 score has been attained. This then has an effect on how the incident is reported which NHS DIGITAL checklist outlines and GMSS must therefore ensure the correct process is followed.

1.2 This document details the Information Governance Incident Reporting process that brings together the various tools that have to be completed when reporting an Information Governance (IG) incident, and/or a Cyber Security incident, including when either such incidents are graded as a SIRI. These reporting processes include the following:

Local GMSS reporting via the tool (DATIX)
Information Governance Toolkit IG Incident Reporting Tool (for IG SIRI's and Cyber Security SIRI's)

1.3 The Incident Reporting Policy and enclosed Procedure is required in order for GMSS to meet its full responsibilities for reporting and managing IG & Cyber Security incidents.

.

2.0 Definitions

2.1 **IG SIRI (Information Governance Serious Incident Requiring Investigation)** – There is no simple definition of a serious incident. What may at first appear to be of minor importance may, on further investigation, be found to be serious and vice versa. As a general guide, the scope of an Information Governance SIRI is as follows:

- The type of incident which will typically breach one of the principles within the current Data Protection Act and Article 6 of the GDPR and / or one of the principles of the Common Law Duty of Confidence.
- Incidents of unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people's privacy.
- Personal data breaches which could lead to identity fraud or have other significant impact on individuals.
- Incidents irrespective of the media involved, which could include both electronic media and paper records relating to staff and service users.

2.1 **IG Cyber SIRI** – There are many possible definitions of what a Cyber incident is. For the purposes of reporting a Cyber-related incident is defined as anything that could (or has) compromised information assets within Cyberspace. It is expected that the type of incidents reported would be of a serious enough nature to require investigation by the organisation. These types of incidents could include:

- Denial of service attacks
- Phishing emails
- Social media disclosures
- Website defacement
- Malicious internal damage
- Spoof websites
- Cyber bullying

3.0 Roles and Responsibilities

3.1 This Incident Reporting Procedure affects the following GMSS roles:

- Managing Director
- Data Protection Officer
- Caldicott Guardian & Deputy
- Senior Information Risk Owner (SIRO) & Deputy
- Information Governance Team
- IT Service Team / IT Security Leads
- Information Security Lead
- DATIX Lead

3.1.1 **Managing Director**
Has ultimate responsibility for the implementation of the provisions of this procedure. As the 'Accountable Officer' they are responsible for the management of the organisation and for ensuring that the appropriate mechanisms are in place to support incident reporting for IG and cyber security incidents.

3.1.2 **Responsibility of the Data Protection Officer (DPO)**
This is a new role required as per the General Data Protection Regulations. The DPO's role is to inform and advise GMSS and its staff about their obligations to comply with the GDPR and other current data protection laws. They are required to monitor compliance with the GDPR and current data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits. In addition they are required to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

3.1.3 **Caldicott Guardian & Deputy**
To review and providing feedback regarding an incident where this relates to patient data. This may involve decision making about informing patients regarding an incident or not if this would deem to cause them harm / distress. To support the delivery of Caldicott principles

3.1.4 **Senior Information Risk Owner (SIRO) & Deputy**
To review IG incidents and report IG and Information Security issues to the Finance Performance & Governance Committee and the Senior Management Team and ensure that any external reporting of the incident, if required, is undertaken.

3.1.5 **GMSS IG Team**

- To co-ordinate and investigate reported IG incidents, maintain IG Incident Logbook, make recommendations and act on lessons learnt.

- To liaise with GMSS IT Security Manager and Information Security Lead as appropriate pertaining to cyber security incidents.
- To escalate incidents to the Head of Integrated Governance, in order to inform the Senior Information Risk Owner / deputy and / or Caldicott Guardian / deputy as appropriate.
- To grade the incident and report it where necessary on the Information Governance Toolkit Incident Reporting Tool, local IG / IG Cyber Security Incident Logbook and DATIX Incident Management System.

3.1.6 **IT Service Team / IT Security Manager**

- For IG Incidents, advise GMSS staff to also report the incident via the DATIX Incident Management System.
- To alert Information Security Lead when a potential or actual cyber security incident is reported.
- To alert the GMSS IG Team when a potential or actual cyber security incident is reported.

3.1.7 **Information Security Lead**

- To work with IT Service Team / IT Security Manager to investigate cyber security incidents, make recommendations and act on lessons learnt
- To liaise with the GMSS IG Team as appropriate especially regarding reporting.
- To inform the Senior Information Risk Owner / deputy and / or Caldicott Guardian / deputy as appropriate.
- To grade the incident, and ensure that where necessary it is reported on the IG Incident Reporting Tool – Cyber Section, local IG / IG Cyber Security Incident Logbook and DATIX Incident Management System (through GMSS IG Team)

3.1.8 **DATIX Lead**

- For all potential and actual IG incidents ask staff to report the incident to the GMSS IG Team via DATIX Incident Management System.
- For cyber security incidents, to ask GMSS staff to report the incident to the IT Service Team / IT Security Manager and the GMSS IG Team.

4.0 IG Incident Reporting & Management Process

4.1 GMSS will continue to utilise its own internal incident reporting procedure for the management of incidents. All incidents must be reported initially via DATIX Incident Management System and if this is identified as an IG incident, this is flagged to the GMSS IG Team. GMSS IG Team will log this on the IG Incident Logbook and assess the incident in the light of GDPR and according to NHS DIGITAL checklist to grade it (Level 1 or below or Level 2 IG SIRI).

4.2 The “Checklist for Reporting, Managing and investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation” is at Appendix 1. This sets out how to grade the severity and sensitivity of an incident.

4.3 All staff are encouraged to report IG *‘near misses’* as well as actual incidents, so that we can take the opportunity to identify and disseminate any *‘lessons learnt’.*

4.4 **Incidents Graded Level 1 or Below**

4.4.1 GMSS utilises its own internal incident reporting procedure for the management of Information Governance incidents graded Level 1 or below – refer to Figure 1 for IG Incident Reporting Process Flowchart.

4.4.2 The incident is graded using NHS DIGITAL grading tool in the "Checklist for Reporting, Managing and investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation" – refer to Appendix 1.

4.5 **Incidents Graded Level 2 or Above (IG SIRI)**

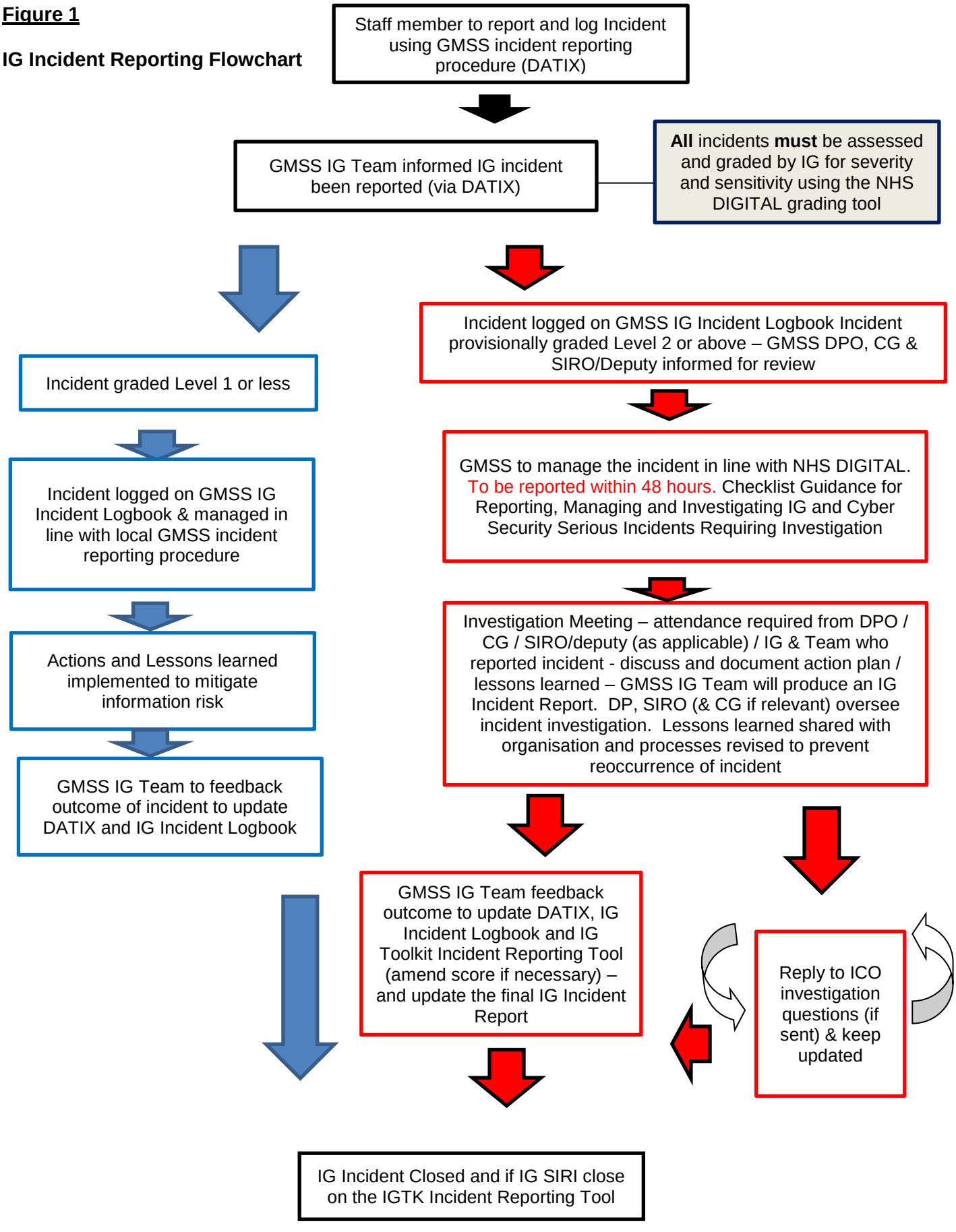
4.5.1 GMSS IG Team will grade the incident utilising its own internal incident reporting procedure as stated above in 4.4.1 and 4.4.2.

4.5.2 Incidents initially graded at Level 2 or above (IG SIRI) are immediately notified to GMSS SIRO and Deputy SIRO, Data Protection Officer / or if appropriate the Caldicott Guardian with a view to them confirming the score.

4.5.3 Once approval has been received from the SIRO/Deputy SIRO, GMSS will report Level 2 incidents on the IG Toolkit Incident Reporting Tool. This must be completed within 48 hours of the incident taking place. In order to do this GMSS IG Team will complete *Information Governance Incident Form for IG SIRIs* – Appendix 2, and use this to report on to the IG Toolkit.

Figure 1

IG Incident Reporting Flowchart



5.0 Cyber Security Incident Reporting and Management Process

5.1 Figure 2 outlines the incident reporting process for cyber security incidents. In most cases, staff will report such incidents via the IT helpdesk as they will tend to be IT related such as PC / laptop not working correctly, phishing emails or denial of access to a system or webpage. Due to this, the IG Team is linking with IT services and GMSS's IT Security Manager to capture such recorded incidents. They will be identified through the use of key words and confirmed whether they are cyber security incidents. The notification of this will be forwarded to the GMSS IG Team who will then liaise with IT Security Manager and Information Security Lead to assess its severity and sensitivity and graded as per NHS DIGITAL checklist. The incident is logged on the Cyber Security Incident Logbook and updated throughout the investigation process.

5.2 Incidents may also be captured via GMSS's incident policy and procedure. In these cases, the GMSS IG Team will liaise with the IT Security Manager and Information Security Lead to inform them and follow the same process as above.

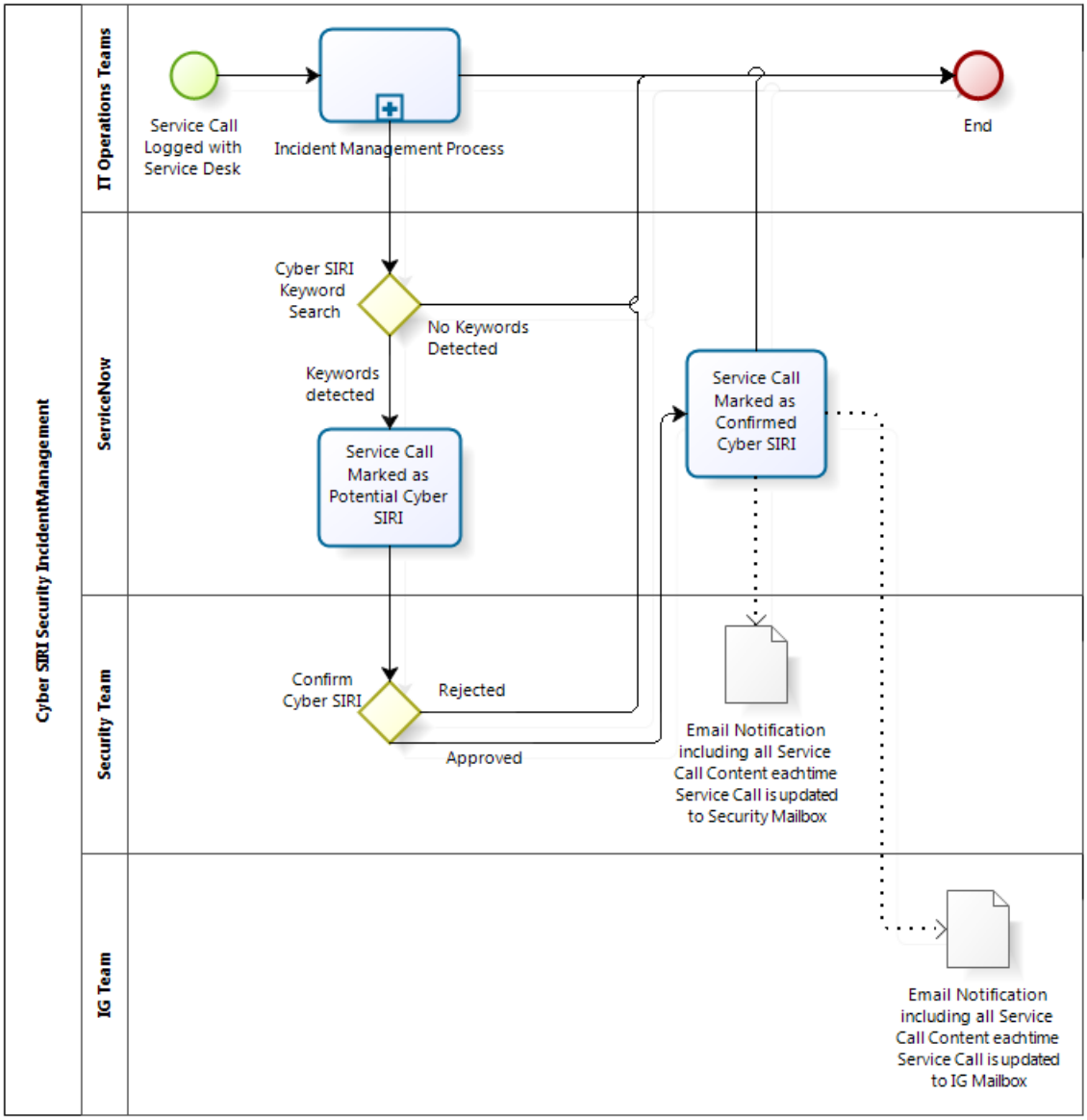
5.3 For Cyber Security incidents, it is vital that the person responsible for any operational response, typically the Head of IT Technical Support is notified and the SIRO / Deputy kept up to date.

5.4 Cyber security incidents scored Level 2 and above must be logged on the IG Toolkit Incident Reporting Tool. This must be completed within 48 hours. This then triggers an automated notification email to the Department of Health and NHS DIGITAL. Please note the ICO are not informed of cyber incidents scored level 2 and above.

Figure 2

Cyber Security Incident Reporting Process

Step One – Notification from IT Services / GMSS IT Security Manager



Step Two – Investigation of Cyber Security Incidents

GMSS IT Team will forward email notification to GMSS IG Team who log incident on GMSS Cyber Security Incident Logbook & inform HoS, IT Tech Support

Follow IG incident investigation process as per Figure 1 liaising with GMSS IT Security Manager / Information Security Lead – note the ICO notification and response is excluded

6.0 Reporting

6.1 Reporting in the Annual Governance Statement / Statement of Internal Control

6.1.1 All IG SIRI's level 2 and above required to be reported will trigger an automated notification email to the Department of Health, NHS DIGITAL and the Information Commissioner's Office, in the first instance, and to other regulators as appropriate.

6.1.2 These incidents need to be detailed individually in the annual report / governance statement / Statement of Internal Control as per Table 1 below. Notes to assist in completion of the table can be found in the NHS DIGITAL checklist (Appendix 1).

Table 1 - Summary table of IG SIRI's

SUMMARY OF SERIOUS UNTOWARD INCIDENTS INVOLVING PERSONAL DATA AS REPORTED TO THE INFORMATION COMMISSIONERS OFFICE [from year to year]				
Date of Incident (month)	**Nature of Incident**	**Nature of data involved**	**Number of people potentially affected**	**Notification Steps**
Jan 2015	*Loss of hardware*	*Forename, Surname, address, NHS number, Medical Details*	*1,500*	*Individuals notified by letter (post)*
Further action on information risk	*GMSS will continue to monitor and assess its information risks, in lights of the events noted above, in order to identify and address any weaknesses and ensure continuous improvement of its systems. The member of staff responsible for this incident has been dismissed.*			

6.2 Reporting to the Senior Management Team

6.2.1 IG incidents are reported routinely at the GMSS IG Group which is a sub-group of SMT via the IG Key Statistics Report. Lessons learned are discussed and actioned when necessary.

7.0 Lessons Learned

7.1 It is essential that action is taken to help to minimise the risk of IG incidents re-occurring in the future. Therefore, all IG incidents that are reported will be logged and any associated lessons learned will be fed back to staff. This may be communicated via email / staff briefings and notices on SharePoint.

7.2 Staff involved with an IG incident should consider with their line manager if additional training and support is needed. Additional training and further information can be gained from NHS DIGITAL Information Governance Training Package, available at:
https://nhsdigital.e-lfh.org.uk/

8.0 Dissemination

8.1 The policy will be disseminated to all Services and can be accessed via the Intranet.

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

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

9.0 Further Information

9.1 Although all staff should know to whom they should report and escalate suspected or actual IG and / or cyber security incidents i.e. via GMSS's local incident reporting procedure and policy, only a number of key members of staff will have the necessary permissions to access the Incident Reporting Appendix of the IG Toolkit. These are:

Information Governance Team
Greater Manchester Shared Services
Phone: 0161 212 6166
Email: gmcsu.igincidents@nhs.net

9.2 Useful Contacts

GMSS Senior Information Risk Owner: SIRO – Julie Daines Julie.daines@nhs.net	**GMSS Caldicott Guardian:** Caldicott Guardian – Andrew White Andrew.white6@nhs.net **Or** Adrienne Bell – Deputy CG adriennebell@nhs.net
GMSS Head of IT Technical Support: Ann Halpin Head of IT Technical Support ann.halpin@nhs.net	

10 Legislation and IG Related Policies

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

A number of other policies are related to this policy and all employees should be aware of the full range below:

- Information Governance Framework
- Information Governance Policy
- Data Protection and Confidentiality Policy
- Information Security Policy
- Acceptable Use Policy
- Records Management Policy
- Information Risk Policy
- Confidentiality Audit Policy
- Information Security Policy

Acts Covered Under Policy

- General Data Protection Regulation
- Data Protection Act

Appendix 1

Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation.

Please click on the link below to view:

https://www.igt. - NHS Digital.gov.uk/resources/ - NHS DIGITAL%20SIRI%20Reporting%20and%20Checklist%20Guidance.pdf