Bolton Clinical Commissioning Group

Information Governance Incident Reporting Policy and Procedure

Policy Number	**IG007**
Target Audience	**CCG/GMSS Staff**
Approving Committee	**CCG Chief Officer**
Date Approved	**February 2018**
Last Review Date	**February 2018**
Next Review Date	**February 2020**
Policy Author	**GMSS IG Team**
Version Number	**V6.0**

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	September 2013	M Robinson D Sankey	Progress to CCG Executive for approval
1	September 2013	CCG Exec	Approved
2	February 2015	D Sankey	Amendment made to reporting process
	February 2015	IM&T Ops Group	Approved
3	Jan 2016	IG Team	Amendment made to include cyber incidents and updates to CCG reporting process via intranet
3	Jan 2016	IM& T Ops Board	Approved
4	Jan 2018	GMSS IG Team	Reviewed and brought in line with GDPR legislation
5	Jan 2018	IM&T Ops Board	Approved
6	Feb 2018	CCG Chief Officer	Approved

Analysis of Effect completed:	By: D Sankey	Date: January 2016

Contents

1 Introduction

Bolton Clinical Commissioning Group (CCG) is committed to a programme of effective risk and incident management. This procedure supports the CCG's Incident Reporting Policy and Procedure and explains the system to be used for staff for the recording, reporting and reviewing of Information Governance (IG) and Information Security (IS) incidents.

The Greater Manchester (GMSS) and CCG have a responsibility to monitor all information governance related incidents that occur that may breach security and / or confidentiality of personal information.

Due to the increase in IG 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 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 the NHS Digital checklist outlines and the CCG must therefore ensure the correct process is followed.

This document details the IG Incident Reporting process that brings together the various tools that have to be completed when reporting an 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 CCG reporting
- Information Governance Toolkit IG Incident Reporting Tool (for IG SIRI's and Cyber Security SIRI's)

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

This procedure applies to all staff who work for or on behalf of the GMSS and CCG. Third party contractors and others (e.g. business partners, including other public sector bodies, volunteers, commercial service providers) who may potentially use the CCG's facilities must be aware of the importance of reporting perceived or actual events.

2 Definitions

Information Governance Related Incident

An information governance or information security related incident relates to breaches of security and / or the confidentiality of personal information which could be anything from users of computer systems sharing passwords, to a piece of paper identifying a patient being found in the high street.

It could also be any event that has resulted or could result in:

- The integrity of an information system or data being put at risk
- The availability of an information system or information being put at risk
- An adverse impact, for example, embarrassment to the NHS, threat to personal safety or privacy, legal obligation or penalty, financial loss and / or disruption of safety or privacy, legal obligation or penalty, financial loss and / or disruption of activities.

Some more common areas of incidents are listed below however this list is not exhaustive and should be used as guidance only. If there is any doubt as to what you have found being an incident it is best to report it to the relevant personnel for this decision:

Breach of security

- Loss of computer equipment due to crime or an individual's carelessness;
- Loss of computer media, for example, cd's, memory sticks/USB sticks due to crime or an individual's carelessness;
- Accessing any part of a database using someone else's authorisation either fraudulently or by accident.

Breach of confidentiality

- Finding a computer printout with personal identifiable data on it in a public area;
- Finding any paper records about a patient / member of staff or business of the organisation in any location outside secured CCG premises;
- Being able to view patient records in an employee's car
- Discussing patient and / or staff personal information with someone else in an open area where the conversation can be overhead;
- A fax being received by the incorrect recipient.

Information Governance Related Serious Incident Requiring Investigation (SIRI)

There is no simple definition of an Information Governance incident. What may at first appear to be a minor issue may, on further investigation, be found

to be serious or vice versa. As a general guide, the scope of an IG SIRI is as follows:

- The type of incident which will typically breach one of the principles within the Data Protection Act 1998 and Article 6 of the General Data Protection Reform (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.

Information Governance Cyber Serious Incident Reporting Investigation (SIR)

There are many possible definitions of what a Cyber incident is. For the purposes of reporting a Cyber-related incident, it 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
- Web site defacement
- Malicious internal damage
- Spoof website
- Cyber bullying.

3 Roles and Responsibilities

Chief Operating Officer
The Chief Operating Officer 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. .

Data Protection Officer (DPO)
This is a new role required as per the General Data Protection Regulations (GDPR). The DPO's role is to inform and advise the CCG 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).

Caldicott Guardian

To review and provide 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.

Senior Information Risk Owner (SIRO)

To review IG incidents and report IG and Information Security issues to the Senior Management Team and ensure that any external reporting of the incident if required is undertaken

Greater Manchester Shared Services (GMSS) Information Governance Team

- To co-ordinate and investigate reported IG incidents, maintain the CCG IG Incident Logbook, make recommendations and act on lessons learnt;
- To liaise with the CCG IG Lead, CCG SIRO and Greater Manchester Shared Services (GMSS) IT Services / Information Security Lead and CCG IT Lead as appropriate pertaining to cyber security incidents;
- To escalate incidents to the CCG IG Lead in order to inform the SIRO, and / or Caldicott Guardian as appropriate;
- To grade the incident and report it where necessary on the IG Toolkit Incident Reporting Tool and update the local CCG IG Incident Logbook.

CCG IT Lead

- To work with IT to investigate the Cyber Security incident, make recommendations and act on lessons learnt;
- To liaise with IG Teams as appropriate especially regarding reporting;
- To inform the Senior Information Risk Owner, and/or Caldicott Guardian as appropriate;
- To grade the incident, and ensure that where necessary it is reported on the IG Incident Reporting Tool – Cyber Security section (through the IG Team).

GMSS IT Services / IT Security Manager

- For IG Incidents, advise CCG staff to report the incident to their CCG IG Lead and GMSS IG Team;
- To alert Information Security Lead and CCG IT Manager 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.

Information Security Lead

- To work with IT Service Team / IT Security Manager / CCG IT 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.

Line Managers

Line managers are responsible for ensuring that all staff, particularly new staff, temporary staff, contractors and volunteers, know what is expected of them with respect to reporting incidents.

CCG Employees

Staff and members are responsible for maintaining the confidentiality of all personal and corporate information gained during their employment term of office with the CCG and this extends after they have left the CCG.

4 Information Governance Reporting and Management Process

The CCG will continue to utilise its own internal incident reporting procedure for the management of incidents:

Staff should report IG and cyber security incidents via the Accident / Incident reporting tool on the Bolton CCG intranet. The link can be found under the "Support" Tab. See Appendix 1 which shows the '*Safeguard'* incident reporting tool, the yellow fields are mandatory.

Reporters can log into the '*Safeguard*' incident reporting tool by entering their CCG user name / password (same details used to access CCG computers).

If a member of staff has no access to the intranet, details should be reported to bolccg.incidents@nhs.net or Tel 462213.

Once an incident has been submitted, an incident number is generated and an email sent to bolccg.incidents@nhs.net.

The immediate response to an incident and the escalation process for investigation or external reporting will vary according to the severity level of the incident.

Where incidents are identified as an IG incident the Governance and Safety Team will liaise with the GMSS IG Team.

GMSS IG Team will log this on the local CCG IG Incident Logbook and assess the incident in the light of GDPR and according to the NHS Digital checklist to grade it (Level 1 or below or Level 2 IG SIRI).

The NHS Digital "Checklist for Reporting, Managing and investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation" is at Appendix 2. This sets out how to grade the severity and sensitivity of an incident.

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'.

Incidents Graded Level 1 or Below

The CCG 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.

The incident is graded using the NHS Digital grading tool in the "Checklist for Reporting, Managing and investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation" – refer to Appendix 2.

Incidents Graded Level 2 or Above (IG SIRI)

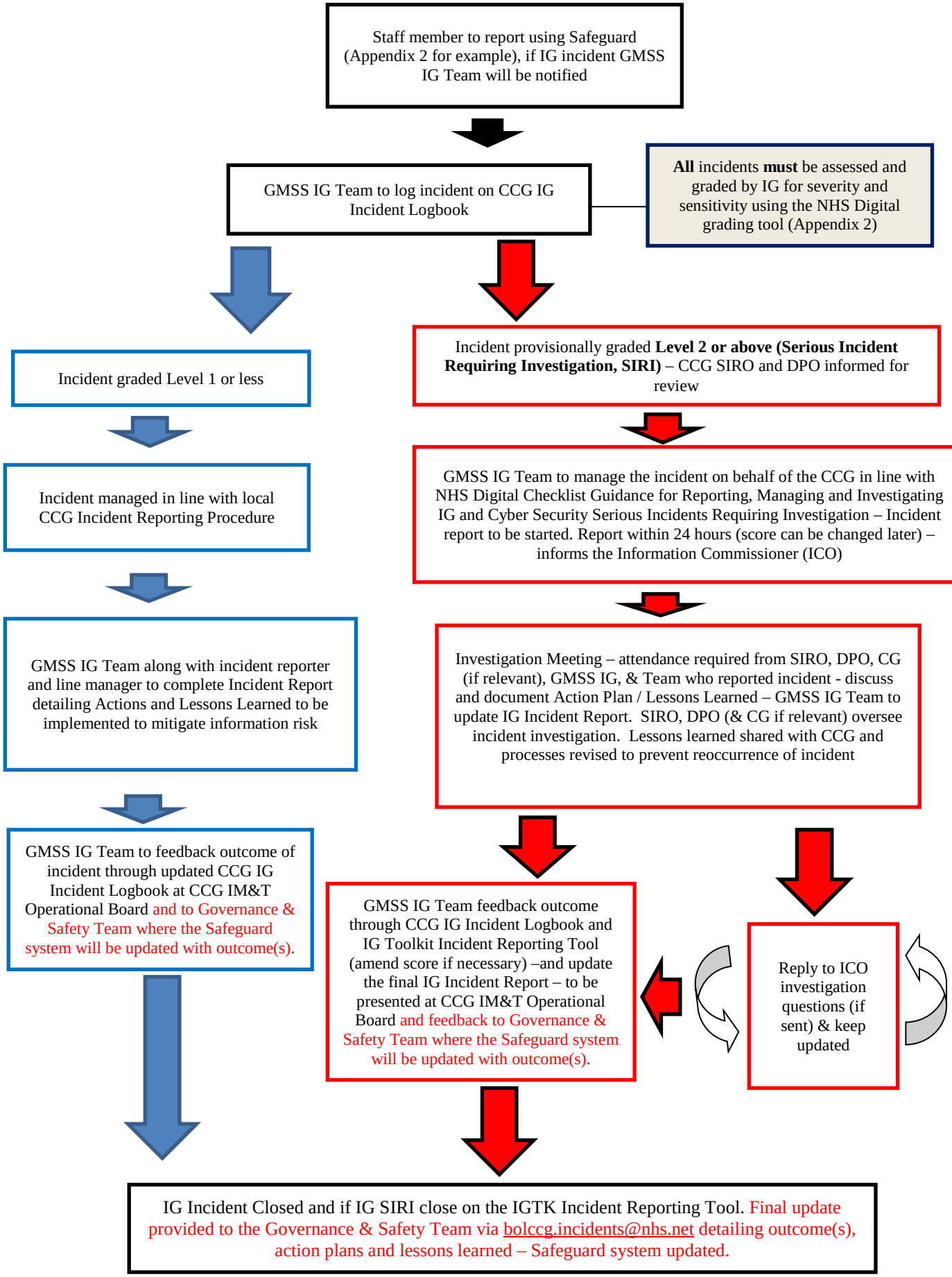
GMSS IG Team will grade the incident utilising the CCG's incident reporting procedure as stated above.

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

Once approval has been received from the SIRO, the GMSS IG Team will report Level 2 incidents on the IG Toolkit Incident Reporting Tool on behalf of the CCG. In order to do this GMSS IG Team will complete the Information Governance Incident Form for IG SIRIs and use this to report onto the IG Toolkit. This must be sent within 24 hours of the incident being reported.

The flowchart (Figure 1) sets out the overall process for reporting, managing and investigating Information Governance incidents for the CCG for incidents scored level 1 and below and level 2 and above (IG SIRI's).

Figure 1 - IG Incident Reporting Flowchart



5 Cyber Security Incident Reporting and Management Process

Figure 2 outlines the incident reporting process for cyber security incidents. In most cases, staff will report such incidents via the GMSS 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 GMSS IG Team are linking with IT services and the GMSS 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 IG Team who will then liaise with IT Security Manager, Information Security Lead and CCG IT Manager to assess its severity and sensitivity and graded as per the NHS Digital checklist. The incident is logged on the Cyber Security Incident Logbook and updated throughout the investigation process.

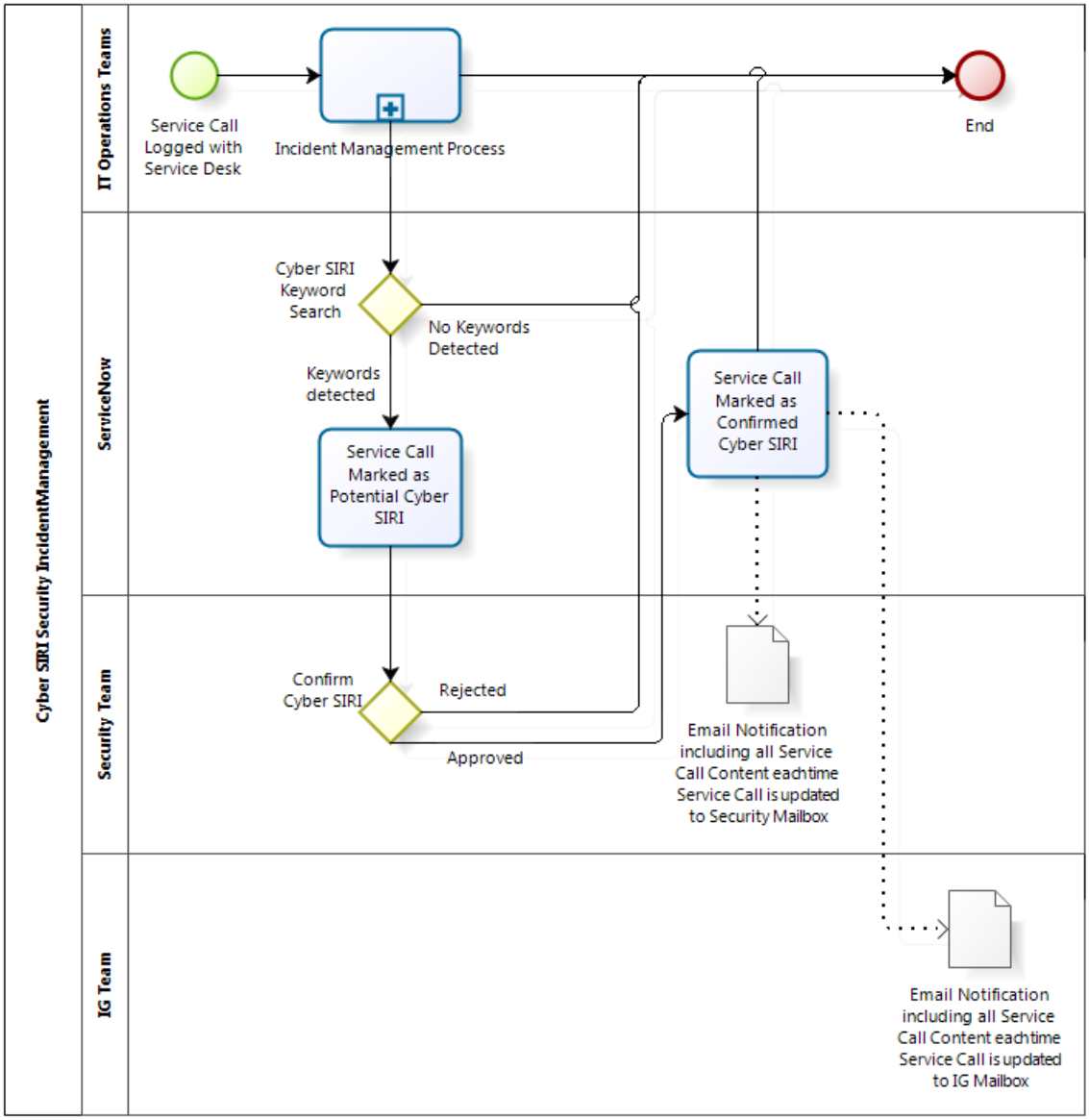
Incidents may also be captured via the CCG's incident policy and procedure. In these cases, the GMSS IG Team will liaise with IT Security Manager, Information Security Lead and CCG IT Manager to inform them and follow the same process as above.

For Cyber Security incidents, it is vital that the person responsible for any operational response, typically the CCG IT Manager is notified and the SIRO kept up to date.

Cyber security incidents scored Level 2 and above must be logged on the IG Toolkit Incident Reporting Tool. 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 CCG Cyber Security Incident Logbook & inform the Information Security Lead, CCG IT Manager and IT Tech Support

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

6 Reporting

Reporting in the Annual Governance Statement / Statement of Internal Control

Incidents classified as IG SIRI's level 2 and above 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.

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 2).

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 2017	*Loss of inadequately protected electronic storage device*	*Forename, Surname, address, NHS number, Medical Details*	*1,500*	*Individuals notified by letter / post*
Further action on information risk	*The CCG 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.*			

A summary of IG incidents can also be published, if the CCG wish to, in annual reports / governance statement using the summary table as highlighted in Table 2:

Table 2 – Annual Summary of IG reported incidents below Level 1

SUMMARY OF OTHER PERSONAL DATA RELATED INCIDENTS IN [insert year to year]		
Category	**Nature of Incident**	**Total**
A	Corruption or inability to recover electronic data	
B	Disclosed in Error	
C	Lost in Transit	
D	Lost or stolen hardware	
E	Lost or stolen paperwork	
F	Non-secure Disposal – hardware	
G	Non-secure Disposal – paperwork	
H	Uploaded to website in error	
I	Technical security failing (including hacking)	
J	Unauthorised access / disclosure	
K	Other	

Please note incidents designated as “pure cyber” are not required to be included in the annual reports and Statement of Internal Control at this time. However cyber incidents that are also IG SIRI’s should be included.

Reporting to the CCG’s Executive Team

IG incidents are reported routinely at the CCG’s IM&T Operational Board Meeting who report to the CCG’s Executive Team. Lessons learned are discussed and actioned when necessary.

7 Closure and Lessons Learned from the IG Incident

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 / team meetings.

Staff involved with an IG incident should consider with their line manager if additional training and support is needed. Line managers should contact the GMSS IG Team for further assistance.

8 Training and Awareness

Line managers are responsible for ensuring that all staff, particularly new staff, temporary staff, contractors and volunteers, know what is expected of them with respect to confidentiality and protecting information. They are also responsible for monitoring compliance with this guideline e.g. undertake ad hoc audits to check for inappropriate disclosures, records left out, abuse of passwords etc.

Staff are responsible for maintaining the confidentiality of all personal and corporate information gained during their employment with the CCG and this extends after they have left the employ of the CCG.

Individual staff members are personally responsible for any decision to pass on information that they may make.

All staff are responsible for adhering to the Caldicott Principles, the Data Protection Act, General Data Protection Regulation and the Confidentiality Code of Conduct.

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

- Policy /strategy and procedure manuals; line manager;
- specific training course;
- other communication methods (e.g. team brief/team meetings); staff Intranet;

All staff are mandated to undertake Information Governance training on an annual basis. This training should be provided within the first year of employment and then updated as appropriate in accordance with the Information Governance policy.

9 Monitoring and review

This procedure will be reviewed every two years or when required due to:

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

10 Legislation and related documents

A set of procedural document manuals will be available via the CCG's website.

Staff will be made aware of procedural document updates as they occur via team briefs, team meetings and notification via the CCG staff Intranet.

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 1998

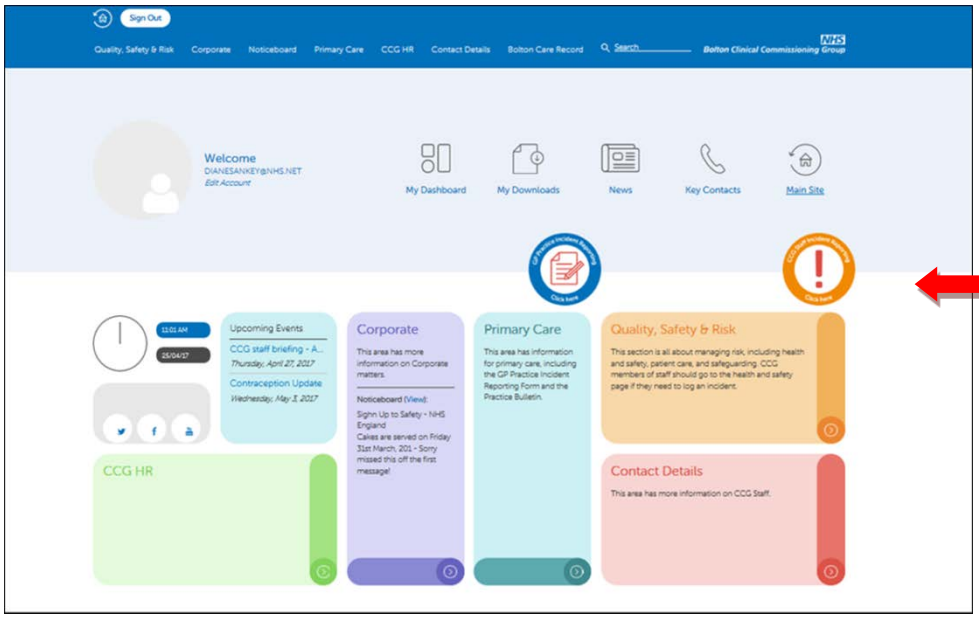
Appendix 1 – How to Log an incident on the Safeguard System

Incidents should be reported via the incident reporting tool ***Safeguard* system** on the intranet.

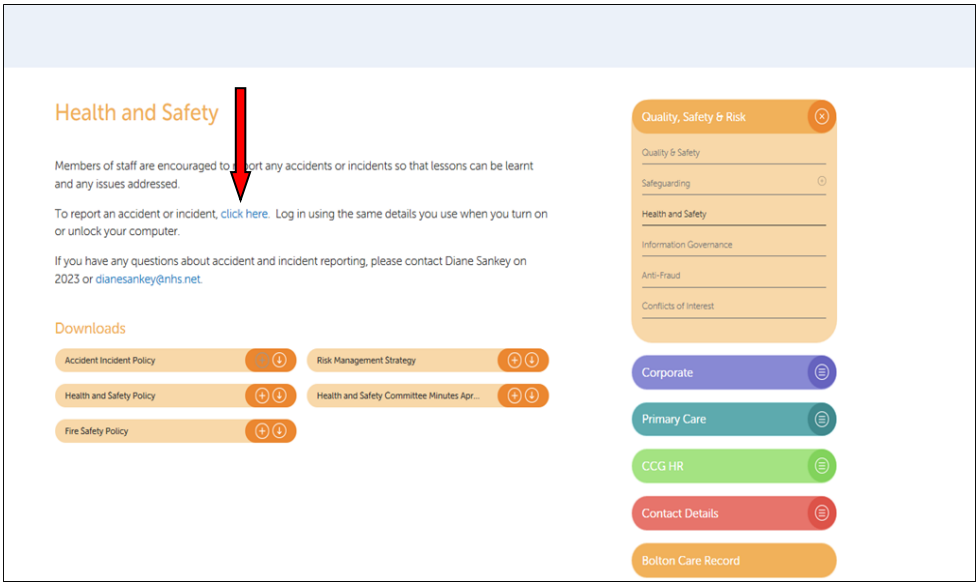
Link to Safeguard Login : http://sgmvmresap78/safeguard/

If you have no access to the intranet, details should be reported to bolccg.incidents@nhs.net or to the Quality & Safety Team, St Peters House on Tel 012404 462213.

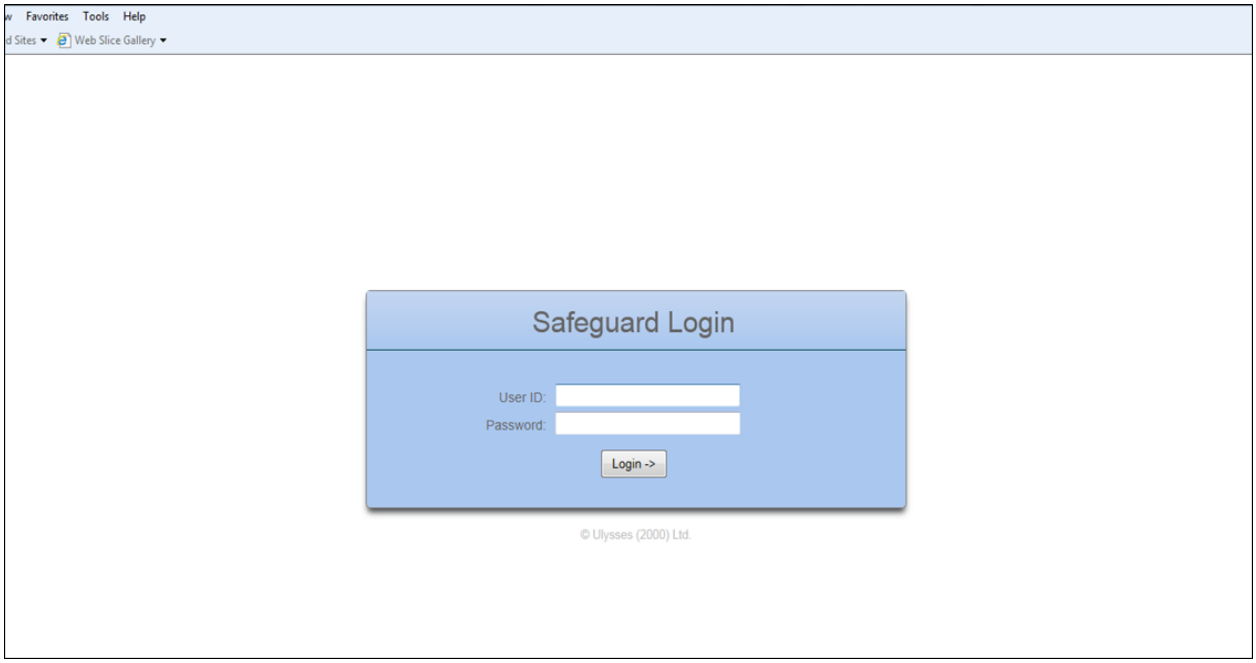
You need to be signed into the CCG intranet



Click

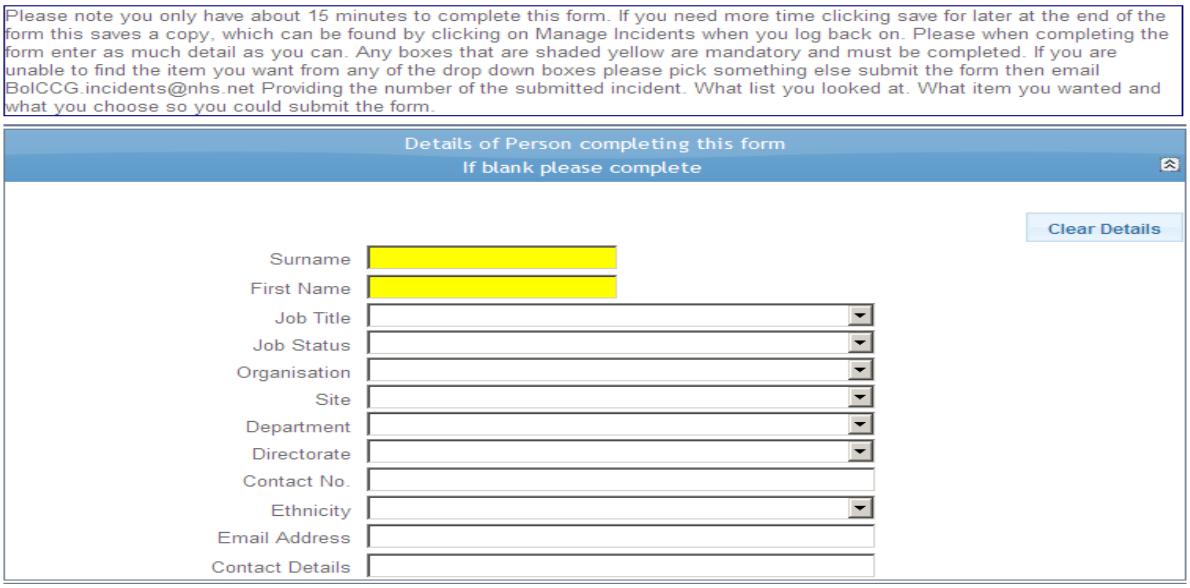


1. **Log into Safeguard System**



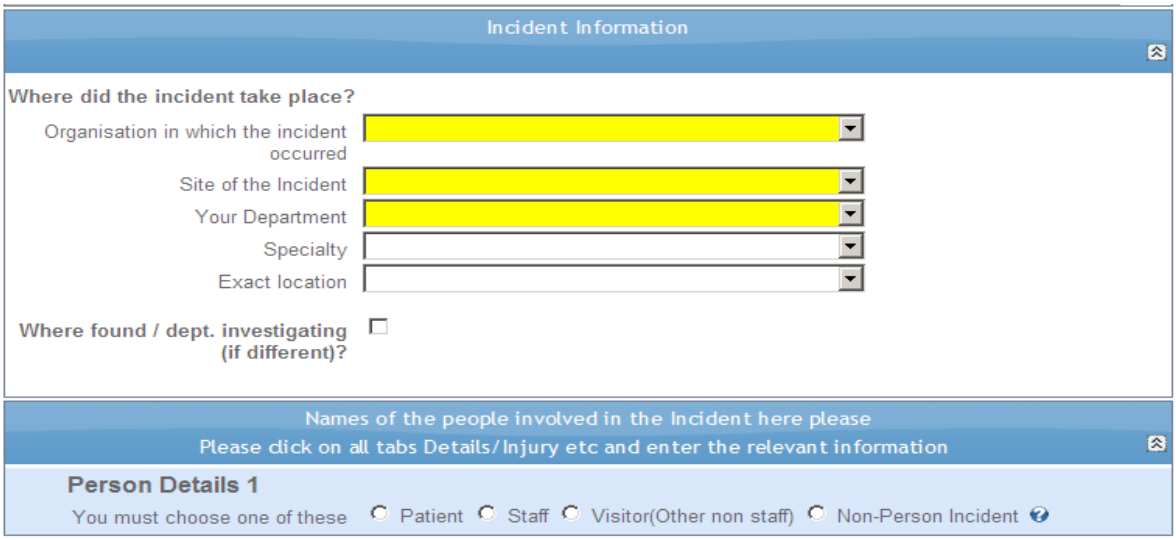
Use your regular user name and password for your computer.

2. Insert or update your details if necessary

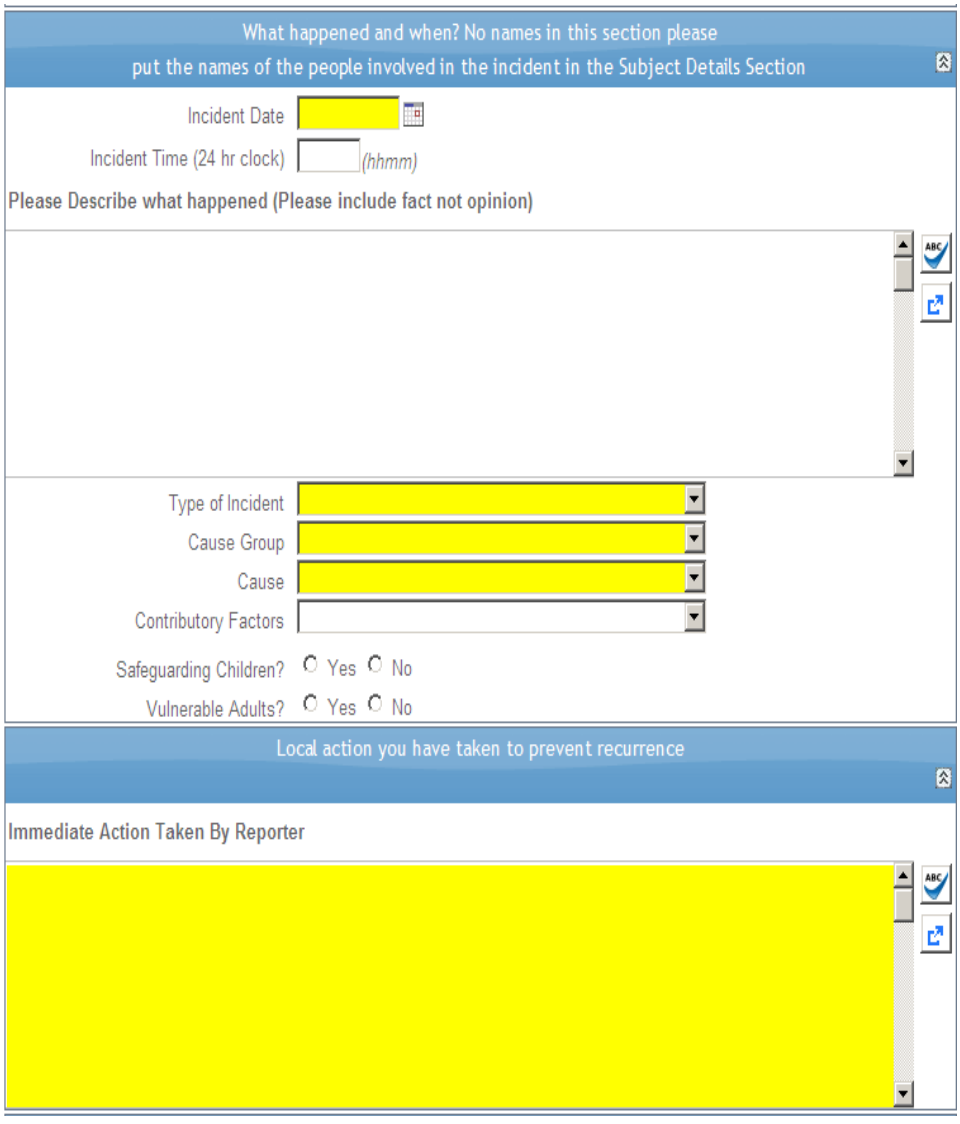


3. Enter data about where the accident/incident occurred, if a person was affected and grade the severity of the event.

   If you or another person was affected, another box will appear for you to add their name and any other relevant identifiable information.



4. Enter accident/ incident date, details of what happened and immediate action taken as a result of the incident.



5. Enter any witnesses to the accident/incident where appropriate.

6. Missing persons or police involvement may be relevant in CHC/safeguarding incidents or if you are reporting violent behaviour.

7. Add any further action you feel should be taken as a result.

8. Enter the name of your line manager who will be notified of the incident.

9. Root Cause Analysis is required for Serious Incidents

10. Click SUBMIT.

11. Once an accident/incident is submitted, you will receive an automated acknowledgement and an incident number for your records.

12. The CCG Risk & Complaints Manager is electronically notified of incidents reported by staff.

13. The Governance and Safety Team will acknowledge receipt of the incident which is shared with CCG managers and other senior leads as appropriate.

    For example:
    - a breach of patient identifiable data (PID) would be notified to Information Governance leads / Caldicott Guardian depending on the severity of the data loss or breach.
    - an incident relating to nursing or CHC funded care is notified to the CCG Chief Nurse and CHC Manager.

14. The immediate response to an incident and the escalation process for investigation or external reporting will vary according to the severity level of the incident.

15. You will receive further feedback if further action is taken to address the issue reported.

16. Key themes/analysis will be reported to various sub-committees or groups within Bolton CCG, learning points discussed and disseminated via:

- Team meetings
- Staff Forum meetings
- Staff bulletins
- Chief Officer Staff briefings

For help and advice, contact Diane Sankey, Liz Mathews and Carol Goodridge on Tel 462213 or email bolccg.incidents@nhs.net.

Appendix 2 - **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

Appendix 3 - Key Contacts

Senior Management Team:
Caldicott Guardian - Dr Jane Bradford
Email: jane.bradford@nhs.net

Senior Information Risk Owner (SIRO) - Ian Boyle
Email: ianboyle@nhs.net

CCG IG Lead - Mike Robinson
Email: Michael.robinson1@nhs.net

CCG IT Lead
Avtar Ubbi
Email: a.ubbi@nhs.net

Governance & Safety Team:
Diane Sankey – Risk & Complaints Manager
Email: dianesankey@nhs.net

Carol Goodridge – Customer Services Officer
Email: c.goodridge@nhs.net

Liz Mathew - Quality & Safety Support Officer
Email: e.mathew@nhs.net

Janet Mitchell – Administrative Assistant
Email: janet.mitchell5@nhs.net
Email: bolccg.incidents@nhs.net

GMSS IG Team:
Caroline Cross – IG Manager
Email: caroline.cross@nhs.net

Camilla Bhondoo – Senior IG Officer
Email: Camilla.bhondoo@nhs.net