NHS
Calderdale
Clinical Commissioning Group

Incident Reporting Policy and Procedure

Policy Ref No: 10

Version/Status:	4.0 / Final
Responsible Committee:	Quality, Finance and Performance Committee
Date Approved:	March 2021
Author:	Corporate Systems Manager
Responsible Lead:	Corporate Systems Manager
Review Date:	March 2023

Version History

Version	Date	Author	Document Status	Commentary: (document development / approval)	Circulation
0.1		Risk, Health and Safety Manager	Draft		Head of Corporate Affairs and Governance
1.0	27/07/17	Risk, Health and Safety Manager	Final	Approved by Quality Committee	All staff via staff workshop, website
2.0	29/11/18	Risk, Health and Safety Manager	Final	Non-material change to IG reporting flowchart. Quality Committee noted the change at its meeting 29/11/18	Website
2.1	19/02/19	Information Governance Manager	Draft	Update of policy to reflect the new NHS Digital guide to the notification of data security and protection incidents	Website
3.0	28/03/19	Risk, Health and Safety Manager	Final	Approved by Quality Committee	Website
3.1	13/01/21	Corporate Systems Manager	Draft		

Version	**Date**	**Author**	**Document Status**	**Commentary: (document development / approval)**	**Circulation**
3.1	01/03/21	Corporate Systems Manager	Draft	Review by IG Team	
4.0	25/03/21	Corporate Systems Manager	Final	Approved by Quality, Finance and Performance Committee	Website, update to staff

Contents

1 Introduction

NHS Calderdale Clinical Commissioning Group (NHS Calderdale CCG) is committed to ensuring that it has an effective incident reporting system in place as part of its Integrated Risk Management Framework. This will enable NHS Calderdale CCG to learn from incidents, share learning and thereby improve safety within the organisation.

Reporting incidents enables the CCG to identify trends and take positive action to prevent or minimise the likelihood of the error or incident recurring in the future. This policy and procedure relate to internal NHS Calderdale CCG incidents and incidents reported by member practices within Calderdale.

This policy and procedure:

- Clarifies roles and responsibilities of staff regarding the management of NHS Calderdale CCG incidents.
- Sets standards regarding investigation and analysis

NHS Calderdale CCG also follows the principles of the Duty of Candour and works to ensure that staff at all levels of the organisation operate within a culture of openness and transparency, understand their individual responsibilities in relation to the duty of candour, and are supported to be open and honest with patients and apologise when things go wrong.

2 Aims and Principles

NHS Calderdale CCG aims to be an organisation with a memory; learning lessons from its incidents and near misses. The objective of this policy is to ensure that NHS Calderdale CCG manages and investigates all reported incidents and near misses in accordance with best practice, learns and shares lessons from them and takes appropriate action to protect staff, contractors, volunteers and members of the public from harm by:

- recording incidents and near misses;
- investigating incidents and identifying root causes;

- regular monitoring of incident data including identifying patterns and trends and appropriate reporting of non-clinical incidents to the Audit Committee and clinical incidents to the Quality, Finance and Performance Committee;
- timely and effective reporting to statutory agencies;
- promotion of a positive culture of reporting and investigation;
- minimising loss of reputation, or assets;
- ensuring that lessons are learned from incidents to prevent such incidents recurring; and
- ensuring that NHS Calderdale CCG complies with current legislation, policies and best practice;
- providing information to the Chief Operating Officer or in their absence the Director of Finance/ regarding incidents where fraudulent activity is suspected. If an investigation is deemed appropriate, the Chief Operating Officer/ or in their absence the Director of Finance will delegate to Calderdale CCG's Local Counter Fraud Specialist (LCFS) who has responsibility for leading the investigation, whilst retaining overall responsibility;
- reporting any personal data breaches that could create a significant risk to the rights and freedoms of an individual to the Caldicott Guardian and incidents and near misses involving staff or other person identifiable data to the Data Protection Officer and Senior Information Risk Owner for assurance that the appropriate steps have been taken in the investigation and learning process.

The principles underlying NHS Calderdale CCG's approach are given below:

2.1 Ensuring Confidentiality

All staff are required to report incidents via DATIX. The incident reporting forms must not include person (patient and staff) identifiable information.

All information relating to incidents will be stored securely in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18) and will conform to NHS Calderdale CCG's Information Governance Policies Book and Procedures Book.

2.2 Just culture

NHS Calderdale CCG is committed to promoting an open, fair and 'just culture' where staff feel able to report incidents or near misses and learn from mistakes without fear of recrimination.

All staff will be encouraged to recognise potential risks and feel supported in the reporting of an event (whether an incident or a near miss) in a just culture.

The CCG adopts a systematic approach to an incident when it is reported and does not rush to judge or 'blame' without understanding the facts surrounding it.

Exceptions to this are where the organisation's policies and guidelines are deliberately breached or there is wilful misconduct or negligence.

2.3 Duty of Candour

NHS Calderdale CCG also follows the principles of the Duty of Candour and believes that all NHS staff must be honest and transparent in what they do in order to best serve and protect patients, staff and visitors to the CCG premises.

2.4 Learning from Incidents

Learning from incidents is critical to the delivery of safe and effective services.

The Audit Committee will receive regular reports relating to corporate incidents, included within its Governance Assurance Report at its meetings occurring three times per year, including root cause analysis outcomes where appropriate.

2.5 Support for staff

Any serious incident is likely to cause concern to the staff involved and affect them profoundly. Each person's experience is different but may include psychological trauma, loss of confidence and feelings of anger, frustration, guilt, loneliness, and isolation – sometimes long after the event. NHS Calderdale CCG is committed to minimising such negative effects, in the interests of individuals and the service. They must be given support and kept fully informed, firstly about the incident, then about the ongoing follow up and investigation of the incident.

3 Scope of Policy

This policy applies to the staff and the Governing Body of NHS Calderdale CCG who are required to report and record sufficient information about an incident, including near misses.

Where an individual fails to comply with this policy action will be taken in line with the Discipline Policy and Procedure.

3.1 References

This policy is one of a set that supports the delivery of the organisation's Integrated Risk Management Framework and should be read in conjunction with the following policies.

NHS Calderdale CCG Policies

- Integrated Risk Management Framework
- Health and Safety Policy
- Fire Safety Policy
- Anti-Fraud, Bribery and Corruption Policy
- Local Security Management Policy
- Safeguarding Children and Adults at Risk Policy
- Whistle Blowing Policy

  IG Policies Book and IG Procedures Book
- CCG Disciplinary Policy and Procedure

This policy and procedure take into account:

- The Health and Safety at Work Act etc. 1974
- The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 2013
- Management of Health and Safety at Work Regulations 1999
- NHS England Serious Incident Framework 2015
- NHS Digital Guide to the Notification of Data Security and Protection Incidents (Sept 2018)
- NPSA 2010 National Framework for Reporting and Learning from Serious Incidents Requiring Investigation

4. Roles and Responsibilities

4.1 Formal Governance and assurance responsibilities

4.1.1 The Governing Body

The Governing Body has responsibility for ensuring a safe and effective risk management and incident reporting system. The Governing Body will monitor incident reporting and management via minutes / reports and assurance from the Audit Committee on a regular basis.

4.1.2 Audit Committee

The Audit Committee is established to assist the Governing Body with the delivery of its delegated responsibilities, including risk management. The Committee has responsibility for maintaining an overview of the adequacy and effectiveness of the integrated risk management system.

The Audit Committee is responsible for monitoring compliance with this policy as part of the overview of the risk management system.

The Audit Committee will review corporate incident reports when it meets three times per year on as part of the Governance Assurance Report. (This is distinct from the performance and management of serious incidents relating to commissioned services reviewed by the Quality, Finance and Performance Committee.)

4.1.3 Quality, Finance and Performance Committee

The Quality, Finance and Performance Committee receives incident reports on an exception basis, for those incidents relating to its area of work i.e. safeguarding or clinical incidents. The Committee also receives quarterly summary reports on incidents reported by member practices.

4.1.4 Counter Fraud in the NHS

The Chief Operating Officer is the Accountable Officer for incidents where fraudulent activity is suspected, and all such information must be reported to them with immediate effect. In the absence of the Chief Operating Officer or Director of Finance such matters must be reported to the Local Counter Fraud Specialist (LCFS) or the National Fraud Reporting line. Further information can be found in the CCG's **Anti-Fraud, Bribery and Corruption Policy** and is available to staff via the intranet.

4.1.5 Local Security Management

A Local Security Management Policy and Procedure is in place.

Staff must notify their line manager and report of any potential security issues including criminal activity incidents to the appropriate manager.

4.2 Individual Responsibilities

4.2.1 Chief Operating Officer

The Chief Operating Officer has overall accountability for risk management and the safety of staff and visitors. The Chief Operating Officer is ultimately responsible for ensuring all investigations are dealt with appropriately.

The Chief Operating Officer is responsible for adherence to this policy, supported by the Corporate Systems Manager. The Chief Operating Officer is also responsible for ensuring that a robust incident reporting process is in place and will, with the support of the Corporate Systems Manager:

- work with colleagues to embed an effective risk management culture throughout the CCG;
- develop a culture of learning lessons from risks, sharing the lessons learned and changing practice as required;
- be responsible for consistently implementing the organisational arrangements for incident reporting throughout the organisation;
- ensure that the serious incident reporting system is maintained
- ensure that all incidents are investigated appropriately in accordance with their severity and are signed off as completed;
- ensure that the processes are in place for the collation of data (quantitative and qualitative) for reporting to the Audit Committee at appropriate intervals, including learning from corporate and clinical incidents;
- ensure arrangements are in place for providing advice to managers in the investigation of incidents; and
- ensure arrangements are in place to offer support to staff during the investigation of incidents.

4.2.2 Chief Operating Officer/Director of Finance

The Chief Operating Officer is the Accountable Officer for incidents where fraudulent activity is suspected and all such information must be reported to the Chief Operating Officer or in their absence the Director of Finance with immediate effect (see paragraph 4.1.4 above).

4.2.3 Senior Information Risk Owner

The Chief Finance Officer is the Senior Information Risk Owner (SIRO) and has organisational responsibility for all aspects of Information Governance, including the responsibility for ensuring CCG has appropriate systems and policies in place to ensure that the organisation has robust Information Governance procedures in place.

The SIRO has a corporate responsibility for overseeing all incidents relating to information governance breaches and ensuring information governance and cyber security serious incidents are reported to regulators in line with NHS Digital's Guide to the Notification of Data Security and Protection Incidents.

4.2.4 Caldicott Guardian

The Caldicott Guardian should be a member of the Governing Body. At NHS Calderdale CCG, this is the Chair of the CCG. The deputy Caldicott Guardian is the Head of Quality. The Caldicott Guardian plays a key advisory role in supporting the CCG to satisfy the highest practical standards for handling patient identifiable information that could create a significant risk to the rights and freedoms of an individual. The Caldicott Guardian will be informed of all incidents relating to patient-identifiable information and the actions being taken to prevent reoccurrence.

4.2.5 Data Protection Officer

The Data Protection Officer (DPO), with the support of the Information Governance Team, is responsible for investigating and reviewing incidents in respect of possible breaches of the UK GDPR and agreeing recommended actions. The DPO will advise the CCG on the reporting of serious incidents, and will be the first point of contact for liaison with the Information Commissioners Office (ICO) in relation to incidents reported to the ICO. The Data Protection Officer for NHS Calderdale CCG is the Chief Finance Officer.

4.2.6 Head of Quality

The Head of Quality has a responsibility for oversight of reported clinical incidents and ensuring the completion of Root Cause Analysis investigations where appropriate as well as dissemination of learning across member practices for clinical incidents.

4.2.7 Corporate Systems Manager

The Corporate Systems Manager has a responsibility for oversight of reported corporate incidents and ensuring the completion of Root Cause Analysis investigations where appropriate, undertaking process reviews as well as the dissemination of learning across the organisation.

The Corporate Systems Manager is also responsible for:

- The management of the incident reporting system, ensuring that CCG staff and member practices are supported with any DATIX related queries, as required
- Ensuring that the electronic risk and incident management systems meet the needs of the CCG
- Supporting the CCG's Quality team in the delivery of member practice reporting including the production of regular analysis and reports into the Quality Committee
- Supporting the IG team in the investigation and reporting of any incidents as required, including health and safety and security incidents (including completion of RIDDOR reports)
- Ensuring local trends are monitored and any areas of concern reported to the appropriate Senior Manager
- Ensuring that staff are briefed in a timely manner on any learning from incidents

4.2.8 Senior Management Team / Line Managers

A member of the senior management team or line managers as appropriate, would usually be the investigating manager (responsible person) (see below) and should acknowledge, investigate, and provide feedback to staff about incidents that have been reported.

Each member of the senior management team is also responsible for ensuring that:

- all staff within their function receive relevant training.
- arrangements are put in place when necessary to support staff who are involved in an incident;
- once advised of an incident will review and compete the relevant section on Datix ensuring the incident has been correctly reported and graded and processed for final approval;
- Compliance with the reporting of information Governance SIRIs (Serious Incidents Requiring Investigation)

- where potentially fraudulent activity is identified as part of the investigation that this is reported to the Chief Operating Officer or in their absence the Director of Finance, the LCFS or through the NHS Fraud and Corruption Reporting Line (0800 028 40 60);
- any learning is shared.

The senior management team is responsible for reviewing the electronic incident forms for their direct reports and processing them for final approval.

4.2.9 Staff

All staff are required to use the online incident reporting form (DATIX) to report incidents. These electronic incident reports are accessible via CCG computers.

All staff should be fully open and co-operative with any investigation process.

Staff are responsible for reporting incidents as soon as possible after the incident (within 48 hours).

5 Definitions and Related Terms

5.1 Near Miss

Any incident which, but for luck or skilful management, would in all probability have resulted in harm to people, property, CCG services or the reputation of NHS Calderdale CCG.

A near miss is different from a ‘no harm’ incident, which is where an incident happened, but no harm resulted (for example, member of staff trips over an object, but the member of staff suffered no injury).

5.2 Incidents

Any accident, event or circumstance that could or did lead to harm,

loss or damage to people, property, reputation, or other occurrence that could

impact on the organisation’s ability to achieve its objectives.

Examples of an incident or near miss may include:

- accidents resulting in harm or injury, however minor;
- loss or damage to equipment;
- all health and safety related incidents;
- physical and/or verbal aggression, assault or abuse;
- security issues including vandalism, criminal damage, theft, fraud or deception;
- information governance incidents including personal data breaches and cyber security incidents.

5.3 Safeguarding Adults and Children at Risk

When dealing with issues/incidents under this policy there should always be a consideration of the potential safeguarding concerns e.g. whether or not an adult at risk or a child has suffered abuse. Should safeguarding concerns be identified a multi-agency safeguarding concern must be raised and the CCG 'Safeguarding Children and Adults at Risk Policy' gives guidance on this. The West Yorkshire Consortium Inter Agency Safeguarding Children Procedures Manual on the consortiums website and the Joint Multi-Agency Safeguarding Adults Policy And Procedures document is located on the Safeguarding Calderdale Website.

5.4 Serious Incidents (SI)

An SI is one where:

- a personal data breach has taken place which meets the threshold for reporting to the ICO as set out within the 'Breach Assessment Grid' within the NHS Digital Guide to the Notification of Data Security and Protection Incidents (Sept 2018) – e.g. inappropriate disclosure of special category data of several hundred patients in response to a Freedom of Information request
- an event has a significant impact on the continuity of essential services under the Network Information Systems (NIS) Regulations 2018 e.g. a cyber security event affecting a wide area network

- a member of staff or member of the public has suffered serious injury, major permanent harm, or unexpected death on health service premises;
- there is a cluster/pattern of incidents or actions by NHS staff which have caused or are likely to cause significant public concern; or
- there is a serious risk to the delivery of the CCG's strategic objectives and/or has the potential to produce significant legal/media or other interest.

An SI may be classified as a 'near miss' incident where the contributory causes are serious and under different circumstances they may have led to a serious incident as above, but no actual harm resulted on that occasion. If it is believed that an incident could be deemed a 'serious incident', the individual or line manager must liaise with the Corporate Systems Manager or the Chief Operating Officer in respect of external reporting systems.

5.5 Health and Safety Incidents

All health and safety incidents must be reported on the DATIX reporting system and the Corporate Systems Manager informed as soon as is reasonably practicable after the incident has occurred. If the incident is categorised as RIDDOR reportable (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013) then an online report will be completed by the Corporate Systems Manager via the Health and Safety Executive website.

5.6 Information Governance Incidents

An information governance related incident refers to the breach, theft or loss of personal confidential data (PCD) of patients or staff. This could be anything from users of computer systems sharing passwords to information containing personal confidential data being sent (e.g. through the post, by fax or e-mail) to the wrong recipient with insufficient security**.**

Information Governance serious incidents are defined as:

- ''…any incident involving the actual loss of personal information that is likely to result in a risk to people's rights and freedoms.''

All information governance breaches should be considered as a potential Information Governance Serious Incident and the management of these will be consistent with the CCG’s Integrated Risk Management Framework and in line with NHS Digital’s Guide to the Notification of Data Security and Protection Incidents (Sept 2018).

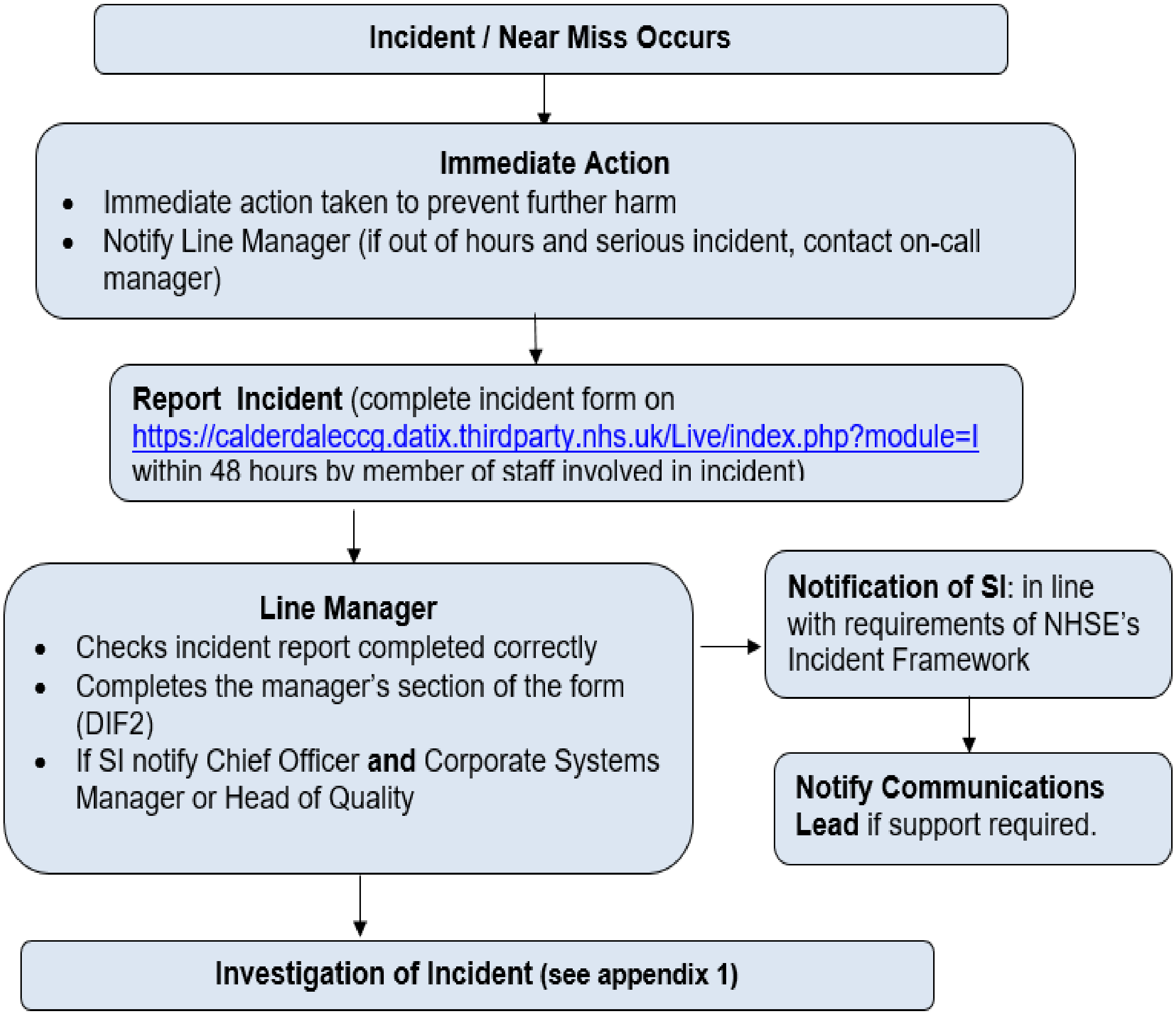
Any personal data breach that could create a significant risk to the rights and freedoms of an individual must be notified to the Information Commissioner via the Data Security and Protection Toolkit reporting tool. The Data Security and Protection Toolkit Incident Reporting Tool provides a breach assessment grid in which the organisation can grade the incident against the likelihood that an adverse effect has occurred and the potential severity of the adverse effect on individuals. All personal data breaches must be reported to Information Commissioner’s Office without undue delay and, where feasible, not later than 72 hours after becoming aware of it unless the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals. If a notification is made after the 72-hour period has expired, the CCG will be required to explain the reasons for the delay.

Staff should refer to NHS Digital’s guidance for further details on types of breaches and severity levels. If in doubt, staff are to seek the advice of the Data Protection Officer, Information Governance Team or the Chief Finance Officer/Deputy Chief Officer (SIRO). Guidance for identifying and managing suspected IG incidents is contained in appendix 3.

All serious personal data breaches that are reportable to the Information Commissioner’s Officer will be reported within the Annual Governance Statement as part of the Annual Report, in line with the requirement set out within the NHS Digital Guide to the Notification of Data Security and Protection Incidents (Sept 2018).

6. Incident Reporting Process

The flowchart below summarises the incident reporting process.



Incident / Near Miss Occurs

Immediate Action

- Immediate action taken to prevent further harm
- Notify Line Manager (if out of hours and serious incident, contact on-call manager)

Report Incident (complete incident form on https://calderdaleccg.datix.thirdparty.nhs.uk/Live/index.php?module=I within 48 hours by member of staff involved in incident)

Line Manager

- Checks incident report completed correctly
- Completes the manager's section of the form (DIF2)
- If SI notify Chief Officer **and** Corporate Systems Manager or Head of Quality

Notification of SI: in line with requirements of NHSE's Incident Framework

Notify Communications Lead if support required.

Investigation of Incident (see appendix 1)

Text description of Incident Reporting Process (as shown in flow chart above)

a) **Incident / Near Miss Occurs.**

b) **Immediate Action:** Immediate action taken to prevent further harm, notify Line Manager (if out of hours and serious incident, contact on-call manager)

c) **Report Incident** (complete incident form on Datix within 48 hours by member of staff involved in incident)

d) **Line Manager:** Checks incident report completed correctly, Completes the manager's section of the form (DIF2), If SI notify Chief Officer and Corporate Systems Manager or Head of Quality.

  i. Notification of SI: in line with requirements of NHSE's Incident Framework

  ii. Notify Communications Lead if support required.

e) **Investigation of Incident** (see appendix 1)

6.1 Complete an Incident Report Form

6.1.1 Complete the on-line DATIX form

6.1.12 Guidance on completing a DATIX incident can be found on the CCG intranet pages

6.2 Incidents reported by / involving stakeholder organisations

6.2.1 Where an incident reported by NHS Calderdale CCG involves an external stakeholder, e.g. another CCG / GP practice, the Corporate Systems Manager will send a copy of the incident form to the relevant risk lead, , requesting that the stakeholder organisation investigates and forwards a copy of their findings to the Corporate Systems Manager

6.2.2 Where an incident is reported to NHS Calderdale CCG by an external stakeholder, e.g. another Trust, the incident will be entered on the Datix system by the Corporate Systems Manager and forwarded to the appropriate CCG member of staff for investigation.

Incidents of any type which may require disciplinary action should also be managed in accordance with the Disciplinary Policy and the HR team should be consulted.

7 Public Sector Equality Duty

An Equality Impact Assessment has been carried out on this policy as it may impact on patients, carers, staff or the wider community. This is attached at Appendix 4.

8 Dissemination and Implementation

NHS Calderdale CCG will ensure that all employees and decision makers are aware of the existence of this policy.

This policy will, following approval by the Quality, Finance and Performance Committee, be disseminated to staff via MS Teams. This will be supported by an awareness session for staff and ongoing support on the use of the online reporting system (DATIX).

All staff will be notified of this policy via the CCG's established communication methods.

9 Monitoring Compliance and Effectiveness

The final review of all electronic incidents by line managers will ensure that investigation and feedback to staff has been carried out.

Monitoring compliance of the policy will be via reports on incident numbers, trends, themes and actions taken to prevent or reduce the likelihood of re-occurrence to the Audit Committee. The Corporate Systems Manager will take any action as necessary.

The Corporate Systems Manager is responsible for ensuring that this policy is reviewed.

10 Archiving

All previous versions of this policy will be stored in a location identified by NHS Calderdale CCG and held in line with record retention and disposal guidelines set out within the IG policies book and IG procedure book.

Appendices

Appendix 1: Incident Investigation Procedure

1 The Level of Investigation

1.1 Not all incidents need to be investigated and analysed to the same extent and should be relative to the incident category (i.e. Red, Amber, Green and Yellow) and whether the incident resulted in harm (i.e. adverse event or near miss) but should follow the investigation protocol. The level of each incident will be determined by the relevant Senior Manager with the support of the Corporate Systems Manager.

1.2 Flowchart – Process for Investigation of Incident

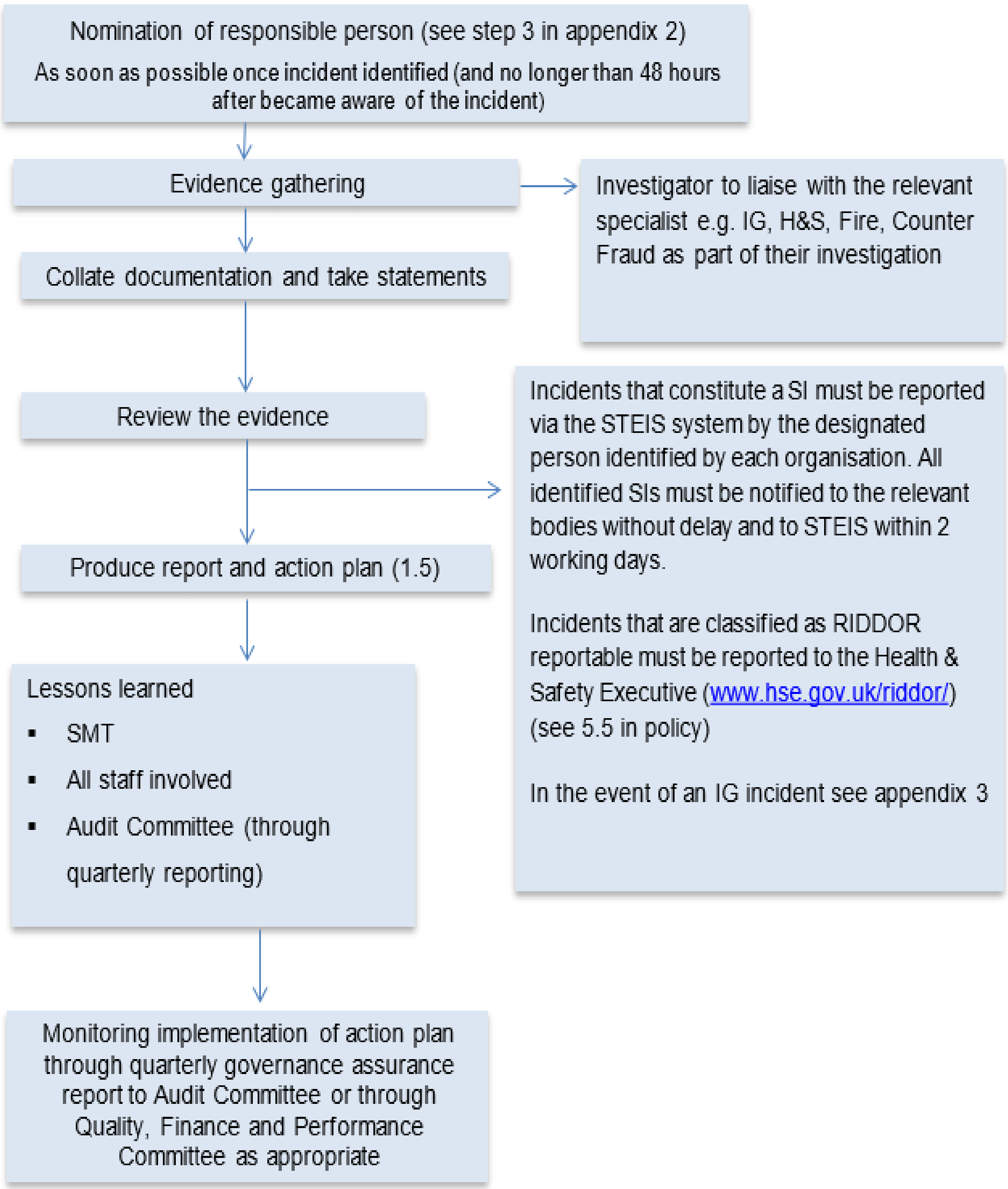
The flowchart on the next page summarises the investigation process to be followed.

The timescale for the investigation will vary depending on the severity of the incident as follows*:

• Red	– up to two months
• Amber	– 1 to 3 days
• Green and Yellow	– up to 5 hours

*See appendix 2 for risk rating of incidents

Flowchart – Process for Investigation of Incident



Nomination of responsible person (see step 3 in appendix 2)

As soon as possible once incident identified (and no longer than 48 hours after became aware of the incident)

Evidence gathering

Investigator to liaise with the relevant specialist e.g. IG, H&S, Fire, Counter Fraud as part of their investigation

Collate documentation and take statements

Review the evidence

Incidents that constitute a SI must be reported via the STEIS system by the designated person identified by each organisation. All identified SIs must be notified to the relevant bodies without delay and to STEIS within 2 working days.

Incidents that are classified as RIDDOR reportable must be reported to the Health & Safety Executive (www.hse.gov.uk/riddor/) (see 5.5 in policy)

In the event of an IG incident see appendix 3

Produce report and action plan (1.5)

Lessons learned

- SMT
- All staff involved
- Audit Committee (through quarterly reporting)

Monitoring implementation of action plan through quarterly governance assurance report to Audit Committee or through Quality, Finance and Performance Committee as appropriate

Text Description of Process for Investigation of Incident (as shown in flow chart)

1.Nomination of responsible person (see step 3 in appendix 2) As soon as possible once incident identified (and no longer than 48 hours after became aware of the incident)

2**.** Evidence gathering: Investigator to liaise with the relevant specialist e.g. IG, H&S, Fire, Counter, Fraud as part of their investigation

3**.** Collate documentation and take statements

4. Review the evidence: Incidents that constitute a SI must be reported via the STEIS system by the designated person identified by each organisation. All identified SIs must be notified to the relevant bodies without delay and to STEIS within 2 working days.

Incidents that are classified as RIDDOR reportable must be reported to the Health & Safety Executive (www.hse.gov.uk/riddor/) (see 5.5 in policy) In the event of an IG incident see appendix 3

5. Produce report and action plan (1.5)

6. Lessons learned:

- SMT
- All staff involved
- Audit Committee (through quarterly reporting)

7. Monitoring implementation of action plan through quarterly governance assurance report to Audit Committee or through Quality, Finance and Performance Committee as appropriate

1.3 Disciplinary action will not form part of the response to an incident, unless one or more of the following applies:

- where, in the view of the NHS Calderdale CCG and/or professional body, the action is significantly removed from acceptable practice;
- where there is a failure to report an incident;
- where a police investigation uncovers criminal activity; or
- where the same individual is at the root or contributor to multiple occurrences of the same incident type.

If disciplinary action is necessary, this will be carried out in accordance with NHS Calderdale CCG's Disciplinary Policy.

1.4 Report and Action Plan

1.4.1 If the investigation relates to a Serious Incident, the responsible person will send the report to the DPO/SIRO/Caldicott Guardian (if IG serious incident), The Corporate Systems Manager and the CCG Quality Team (which has lead responsibility for SIs) to review the investigation and provide quality assurance on submitted documents.Any request for further information or agreed closure will be communicated to the Responsible Person (see step 3 in Appendix 2).

1.4.2 The relevant Head of Service and investigating manager is responsible for ensuring that action plans are delivered on time and that all reports pertinent to these action plans are presented to the appropriate overseeing committee in a timely manner. They may delegate responsibility for specific action plans to members of their team.

Appendix 2: Guidance for risk rating of incidents

All incidents should be graded according to the severity of outcome and the likelihood of occurrence as soon as possible after the event.

The risk score can help us decide what level of investigation is required. The actions that take place as a result of the investigation should then reduce the harm and/or likelihood of the incident occurring again.

Step 1 - Risk Consequence

The Risk Consequence rating refers to the impact that the incident would have. On DATIX this is shown as follows:

Physical and Mental Injury to a Person

Consequence	Examples
1 - None, No injury	No obvious injury. No treatment required. No time off work (for staff incidents).
2 - Minor Injury soft (sprain)	Small cut, bruise or sprain. First Aid is required. Three or less days off work (for staff incidents).
3 - Moderate Injury (fracture)	Reportable to external agencies and/or statutory bodies (e.g. RIDDOR, HSE, NPSA). Medical intervention required. 4-14 days off work (for staff incidents). Semi-permanent disablement.
4 - Major, Serious Permanent Injury	Major injuries, long term incapacity or disability. Single permanent injury. More than 14 days off work.
5 - Catastrophic, Very Serious (death)	Fatality or multiple permanent injuries. Lifelong disablement.

Adverse Publicity/Reputation

Consequence	Examples
1 - None, No injury	No media interest.
2 - Minor Injury soft (sprain)	Low local newspaper interest.
3 - Moderate Injury (fracture)	High local media interest. Local MP interest.
4 - Major, Serious Permanent Injury	Regional media coverage. National Media coverage of less than 3 days.
5 - Catastrophic, Very Serious (death)	Ministerial enquiry. Full public enquiry.

Information Governance (Breach of Confidentiality)

Consequence	Examples
1 - None, No injury	Near Miss.
2 - Minor Injury soft (sprain)	Single failure to protect personal data or provide access to information.
3 - Moderate Injury (fracture)	Repeated failure to protect personal data or provide access to information.
4 - Major, Serious Permanent Injury	Significant risk to the rights and freedoms of the individual that triggers notification to ICO or failure to meet national standards affecting external assessment rating.
5 - Catastrophic, Very Serious (death)	Information Commission or Tribunal investigation.

Financial

Consequence	Examples
1 - None, No injury	Small loss (less than £1,000).
2 - Minor Injury soft (sprain)	Loss between £1,000 and £100,000.
3 - Moderate Injury (fracture)	Loss of more than 0.1% of the budget or between £100,000 and £250,000.
4 - Major, Serious Permanent Injury	Loss of more than 0.25% of budget or between £250,000 and £1 million.
5 - Catastrophic, Very Serious (death)	Loss of more than 1% of budget or more than £1 million.

Step 2 - Risk Likelihood

The Risk Likelihood rating refers to the likelihood that the incident will reoccur. On Datix this is shown as follows:

Likelihood of recurrence

5 – Almost certain (likely to occur every 4 weeks or more (100% chance to recur)

4 – Likely (Likely to occur in a six-month period)

3 – Possible (Likely to occur yearly)

2 – Unlikely (Likely to occur once in a 3-year period)

1 – Rare (Unlikely to occur again)

Step 3 - Risk Assessment Rating Matrix

Plotting the consequence and likelihood of the incident on the Risk Matrix will give you a risk score (consequence x likelihood = risk rating).

Risk Assessment rating matrix

Please note this may not be accessible for all users please request an accessible version if needed.

Plotting the consequence and likelihood of the incident on the Risk Matrix will give you a risk score (consequence multiplied by likelihood equals risk rating).

Risk Grading	**Consequence**	**Consequence**	**Consequence**	**Consequence**	**Consequence**
Likelihood of recurrence	**Insignificant (1)**	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Catastrophic (5)**
Almost certain (5)	🟨	🟧	🟥	🟥	🟥
Likely (4)	🟨	🟧	🟧	🟥	🟥
Possible (3)	🟩	🟨	🟧	🟧	🟥
Unlikely (2)	🟩	🟨	🟨	🟧	🟧
Rare (1)	🟩	🟩	🟩	🟨	🟨

Key to Table showing level of risk

Green	Low risk	**Yellow**	Moderate risk	**Orange**	High risk	**Red**	Serious risk incident

Nomination of 'Responsible' Person to Lead Investigations.

(Green) Low Risk Incidents (scored 1-3)

It is unlikely that a formal investigation will have to be undertaken on these types of incidents. The DATIX report should be updated with any actions or lessons learned from the incident.

(Yellow) Moderate Risk Incidents (scored 4-6)

It is unlikely that a formal investigation will have to be undertaken on these types of incidents. The DATIX report should be updated with any actions or lessons learned from the incident.

(Orange) High Risk Incidents (scored 8-12)

The appropriate team manager will identify an appropriate member of their team to undertake the investigation. The Manager should be supported where necessary by the Corporate Systems Manager. If they have not had the necessary training in root cause analysis techniques, this support can be accessed from the Corporate Systems Manager.

(Red) Serious Risk Incidents (scored 15-25)

An appropriate Head of Service as nominated by the Chief Operating Officer, will lead the investigation of incidents deemed “high”, supported by the Corporate Systems Manager. Guidance on the root cause analysis process can be given by trained staff e.g. the Corporate Systems Manager.

Appendix 3: Guidance for Identifying and Managing Suspected Information Governance Incidents

In the event of an incident occurring of an Information Governance breach, please refer to the Information Governance policies book in the first instance and notify the Corporate Systems Manager or the CCG Information Governance Team for advice and support.

1. Introduction

All incidents and near misses relating to Information Governance should be reported following the DATIX incident reporting procedure in appendix 1.

2. What is an Information Governance Related Incident?

An information governance incident includes, but is not limited to, any violation of the organisations Information Governance policies. An information governance related incident may relate to the breach, theft or loss of personal confidential data (PCD), of patients, staff or other identifiable individuals. This could be anything from users of computer systems sharing passwords to an email containing personal confidential data being sent to the wrong recipient with insufficient security to protect the message.

Information Governance incidents cover:

- Loss or potential loss of Personal Data/Information
- Breach of Confidentiality and unauthorised disclosure of person identifiable information
- Inappropriate use/access or loss of access to personal information
- Recording or sharing of inaccurate data
- Inappropriate invasion of people's privacy
- Breaches which could lead to identity fraud or have other significant impact on individuals
- unauthorised or accidental alteration of personal data

- Cyber security incidents e.g. key logging, denial of service attacks

Examples of Information Governance incidents that should be reported (list not exhaustive):

- Finding personal confidential data (PCD) left unattended e.g. printer/photocopier machine;
- Discovering that a fax containing PCD has been received/sent to an incorrect recipient
- An email containing PCD received/sent to the wrong person or sent using unencrypted email.
- Losing an equipment that may hold personal information on it;
- Giving information to someone who should not have access to it – verbally, in writing or electronically;
- Accessing a computer database using someone else's authorisation e.g. someone else's user id and password, smartcard;
- Sending a sensitive e-mail to 'all staff' by mistake;
- Finding a colleague's password written down on a 'post-it' note;
- Discovering a 'break in' to the organisation.
- Threat of cyber security e.g. hacking, threats to servers and data
- Finding confidential waste in a 'normal' waste bin.
- PCD being held inadequately secure e.g. on hard drives, shared drives, unlocked cabinets
- Anonymised data that is discovered to contain hidden fields or links to personal/confidential information.

Please note that the loss or theft of removable media (including laptops, removable discs, CDs, USB memory sticks, PDAs and media card formats) upon which data has been encrypted to the approved standard, is not a Serious Untoward Incident unless you have reason to believe that the protections have been compromised or were improperly applied.

Further examples of breach types are available from Appendix 5 of the NHS Digital Guide to the Notification of Data Security and Protection Incidents (Sept 2018).

3. Process for reporting IG Incidents*

Any security breach that creates a risk to the rights and freedoms of the individual is a personal data breach and could be notifiable to the ICO if it reaches a certain threshold. Initially the incident is to be reported using the CCG's incident reporting template (via DATIX). If it is established that the incident is IG related, the Information Governance Lead (Corporate Systems Manager) will be notified that an IG incident has occurred. The severity of the incident should be established at the earliest opportunity as well as identifying who the owner/s of the data are and identifying the relevant parties to be informed of the incident.

The likelihood that an adverse effect has occurred and the potential severity of the adverse effect on individuals involved, should be assessed in line with the grading process set out within the NHS Digital guide.

Where an incident is found to meet the threshold for reporting to the ICO as set out in the 'Breach Assessment Grid' within the NHS Digital Guide to the Notification of Data Security and Protection Incidents, then it must be reported through the Data Security and Protection Toolkit (DSP Toolkit) Incident Reporting Module, with which the organisation can grade the incident to see whether it does meet the criteria of a reportable data breach e.g. high profile incidents involving a breach of the Data Protection Act or Common Law Duty of Confidentiality, and are reportable to the Department of Health and the Information Commissioner's Office. The Information Governance Team has access to the DSPT Toolkit and will assist the Data Protection Officer in the reporting process.

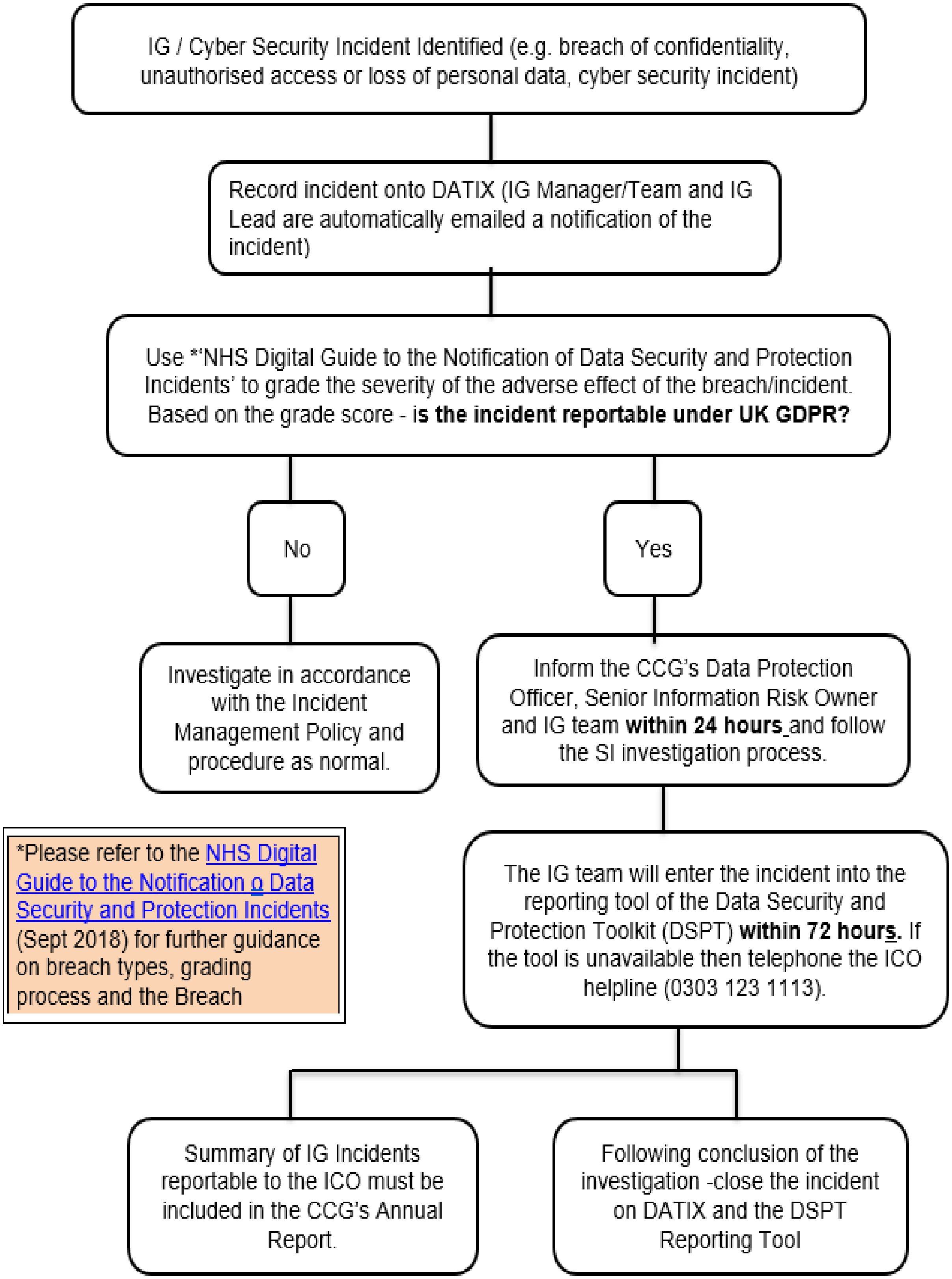
Reporting of the incident on the Data Security and Protection Incident Reporting Tool must take place within 72 hours of becoming aware of the incident.

The Department of Health and Social Care will also be notified where it is (at least) likely that harm has occurred, and the impact is at least serious. It is advised that these incidents are reported on the Data Security and Protection Incident Reporting Tool within 24 hours of becoming aware of the incident.

For Information Governance incidents a root cause analysis investigation should be undertaken and appropriate input from relevant subject matter experts, Information Governance, ICT, IT Security, Risk etc. Process reviews of information governance related incidents and near misses will be undertaken at least once a year. The review meetings is part of the process of identifying and improving processes.

Reference should also be made to the Disciplinary Policy, and the HR team should be contacted, to establish whether the breach may also require investigation under the Disciplinary Policy.

Flowchart for the process for reporting IG incidents



IG / Cyber Security Incident Identified (e.g. breach of confidentiality, unauthorised access or loss of personal data, cyber security incident)

Record incident onto DATIX (IG Manager/Team and IG Lead are automatically emailed a notification of the incident)

Use *'NHS Digital Guide to the Notification of Data Security and Protection Incidents' to grade the severity of the adverse effect of the breach/incident. Based on the grade score - **is the incident reportable under UK GDPR?**

Investigate in accordance with the Incident Management Policy and procedure as normal.

Inform the CCG's Data Protection Officer, Senior Information Risk Owner and IG team **within 24 hours** and follow the SI investigation process.

*Please refer to the NHS Digital Guide to the Notification o Data Security and Protection Incidents (Sept 2018) for further guidance on breach types, grading process and the Breach

The IG team will enter the incident into the reporting tool of the Data Security and Protection Toolkit (DSPT) **within 72 hours.** If the tool is unavailable then telephone the ICO helpline (0303 123 1113).

Summary of IG Incidents reportable to the ICO must be included in the CCG's Annual Report.

Following conclusion of the investigation -close the incident on DATIX and the DSPT Reporting Tool

Text description of the flowchart showing the process for reporting IG incidents

1.IG / Cyber Security Incident Identified (e.g. breach of confidentiality, unauthorised access or loss of personal data, cyber security incident

2. Next Record incident onto DATIX (IG Manager/Team and IG Lead are automatically emailed a notification of the incident)

3. Use *'NHS Digital Guide to the Notification of Data Security and Protection Incidents' to grade the severity of the adverse effect of the breach/incident. Please refer to the NHS Digital Guide to the notification of Data Security and Protection incidents Sept 2018 for further guidance on breach types, grading process and breach assessment grid.

Based on the grade score - i**s the incident reportable under UK GDPR?**

If **No** Investigate in accordance with the Incident Management Policy and procedure as normal.

If **Yes**

1. Inform the CCG's Data Protection Officer, Senior Information Risk Owner and IG team within 24 hours and follow the SI investigation process.
2. The IG team will enter the incident into the reporting tool of the Data Security and Protection Toolkit (DSPT) within 72 hours. If the tool is unavailable, then telephone the ICO helpline (0303 123 1113).
3. Following conclusion of the investigation -close the incident on DATIX and the DSPT Reporting Tool
   Summary of IG Incidents reportable to the ICO must be included in the CCG's Annual Report.

Appendix 4: NHS Calderdale CCG Equality Impact Assessment

Title of policy: Incident Management Reporting Policy and Procedure

Names and roles of people completing the assessment: Rob Gibson, Corporate Systems Manager

Date assessment reviewed: January 2021

1. Outline

Give a brief summary of the policy

The objective of this policy is to ensure that NHS Calderdale CCG manages and investigates all incidents in accordance with best practice, learns and shares lessons from them and takes appropriate action to protect patients, staff contractors, volunteers and members of the public from harm

What outcomes do you want to achieve?

To ensure that there is clear accountability and effective processes in place for the reporting, investigation and management of incidents.

2. Analysis of impact

This is the core of the assessment, using the information above detail the actual or likely impact on protected groups, with consideration of the general duty to eliminate unlawful discrimination; advance equality of opportunity; foster good relations

Characteristics	**Are there any likely impacts?** **Are any groups going to be affected differently?** **Please describe.**	**Are these negative or positive?**	**What action will be taken to address any negative impacts or enhance positive ones?**
Age	No		

Characteristics	Are there any likely impacts? Are any groups going to be affected differently? Please describe.	Are these negative or positive?	What action will be taken to address any negative impacts or enhance positive ones?
Carers	No	N/A	N/A
Disability	No	N/A	N/A
Sex	No	N/A	N/A
Race	No	N/A	N/A
Religion or belief	No	N/A	N/A
Sexual orientation	No	N/A	N/A
Gender reassignment	No	N/A	N/A
Pregnancy and maternity	No	N/A	N/A
Marriage and civil partnership	No	N/A	N/A
Other relevant group	No	N/A	N/A

3. If any negative/positive impacts were identified are they valid, legal and/or justifiable? Please detail.

None identified. Having considered this policy it is felt that there are unlikely to be any potential positive or negative impact.

4. Monitoring, Review and Publication

How will you review/monitor the impact and effectiveness of your actions

Review of policy on regular basis and update of equality impact assessment accordingly.

Lead Officer: Rob Gibson

Review date: January 2023

If you have identified a potential discriminatory impact of this procedural document, please refer it to Sarah Mackenzie-Cooper, Equality and Diversity Manager, together with any suggestions as to the action required to avoid/reduce this impact.

For advice in respect of answering the above questions, please contact the Equality and Diversity Lead