NHS
Northumberland
Clinical Commissioning Group

Corporate	**CCG CO08 Incident Reporting and Management Policy**

Version Number	**Date Issued**	**Review Date**
V3.2	January 2021	January 2023

Prepared By:	Elizabeth Durham, Senior Governance Officer, NECS
Consultation Process:	Governance Team, NECS Clinical Quality Team, NECS Heads of Customer Relations, NECS Business Information Services, NECS NHS Northumberland Clinical Commissioning Group
Formally Approved:	13 January 2021

Policy Adopted From:	CO08 Incident Reporting and Management Policy v3.1
Approval Given By:	Clinical Management Board

Document History

Version	**Date**	**Significant Changes**
1	28/02/2013	Policy provided to Clinical Commissioning Group (CCG) as part of policy suite
2	03/02/2015	Policy rewrite in line with changing CCG incident reporting and management requirements aligned to the introduction of Safeguard Incident Risk System (SIRMS) across the CCG.
3	May 2018	Revised NHS police and reference documents. Added Cyber and GDPR.
3.1	July 2020	Extension request in light of COVID19 pandemic. No impact on external environment factors nor legislation updates identified.
3.2	January 2021	Updates to: definitions, fraud section, further clarification provided on IG incidents, further clarification on the role of NECS Clinical Quality team, roles and responsibilities reviewed, Equality Impact screening template updated. All procedural appendices removed into CCG Incident Reporting and Management User Guide.

Equality Impact Assessment

Date	Issues
January 2021	See section 12 of this document

POLICY VALIDITY STATEMENT

This policy is due for review on the latest date shown above. After this date, policy and process documents may become invalid.

Policy users should ensure that they are consulting the currently valid version of the documentation.

Accessible Information Standards

If you require this document in an alternative format, such as easy read, large text, braille or an alternative language please contact norccg.enquiries@nhs.net

Contents

Contents

1. Introduction

The Clinical Commissioning Group (CCG) aspires to the highest standards of corporate behaviour and clinical competence, to ensure safe, fair and equitable procedures are applied to all organisational transactions, including relationships with patients and their carers, the public, staff, stakeholders and use of public resources. In order to provide clear and consistent guidance, CCG will develop documents to fulfil all statutory, organisational and best practice requirements.

The CCG has a responsibility for managing incidents to ensure the quality of the services it commissions is safe and of a high standard. The CCG has a responsibility to ensure their contractors have effective systems in place to identify and manage incidents and risks and support them in their development where necessary.

In our duties as a CCG we are required to act as a conduit for information about such risks and incidents and to ensure that the learning (and the opportunities for risk reduction) from them is not lost within the CCG or the wider NHS.

This policy sets out the CCG's approach to the management of incidents in fulfilment of its strategic objectives and statutory obligations.

The reporting of incidents will help the CCG identify potential breaches in its core business including breaches in:

- Contractual obligations
- Internal processes
- Performance targets
- Service specifications etc.
- Statutory duties

This policy will enable the organisation to learn lessons from adverse events and supports implementation of action to prevent incidents reoccurring. Reported incidents will be periodically analysed and results will be shared with directorates, departments and stakeholders where appropriate. The reporting and management process uses a root cause approach to analyse incidents.

The CCG aims to develop an open learning culture of incident reporting, based on the principles of fair blame.

This policy covers the broad categories as follows:

- Corporate business incidents
- Health and safety / fire / security or environmental incidents
- Information Governance Incidents
- IT (Information Technology) Incidents
- Clinical quality incidents

The policy interlinks with CCG CO18 Serious Incidents Management Policy.

The adoption and embedding within the organisation of an effective integrated incident management framework will ensure that the reputation of the CCG is maintained, enhanced, and its resources used effectively to ensure business success, financial strength and continuous quality improvement in its operating model.

1.1 Status

This is a corporate policy and outlines the Incident Reporting and Management Framework for Northumberland Clinical Commissioning Group.

1.2 Purpose and scope

This policy provides information and guidance to staff working within the CCG to report incidents and near misses. This will be achieved by:

- Setting out the principles on the process for reporting and managing incidents (for both CCG employees and contractors) including the use of the Safeguard Incident and Risk Management System (SIRMS);
- Setting out the roles and responsibilities of CCG employees, contractors committees and the organisation as a whole in the reporting and management of incidents;
- Outlining the principles that underpin the organisation’s approach to incident reporting and management;
- Providing clear definitions of the terminology within incident reporting and management;
- Providing clear guidance to employees of the organisation as to the kinds of incidents and issues that can be reported within the system;
- Providing a clear organisational position on the principles of investigation used when responding to incidents, including fair blame and root cause analysis;
- Outlining how actions, outcomes, trends and lessons learned from incidents will be monitored and reviewed;
- Providing information and guidance on how the organisation aims to meet the requirements for onward reporting of incidents to the National Reporting and Learning System (NRLS) and Serious Incident to the Strategic Executive Information System (StEIS); and
- Integrating where relevant the existing organisational policy for Serious Incidents (SIs) **“CCG CO18 Serious Incidents (SIs) Management Policy**”.

2. Definitions

2.1 Definition of an Incident

An incident is a single distinct event or circumstance that occurs within the organisation which leads to an outcome that was unintended, unplanned or unexpected.

The incident could also occur outside the organisation if a member of staff is visiting other locations in the course of their work.

Incidents are often negative by nature but can also include positive leaning events which can be shared throughout the organisation as good practice.

An incident could involve:

- Environment (workplace)
- Organisational reputation
- Property
- Service delivery
- Staff
- Stakeholder

The incident might impact on different aspects of CCG operations for example:

- Reputation
- Resources
- Staff
- Quality of services

2.2 Glossary of Terms

The following terms are used in this document:

A Business Continuity Incident
An unwanted event that threatens personnel , buildings, operational procedures or the reputation of the organisation which requires special measures to be taken to restore things back to normal.
Note: This is not a separate category in itself because these types of incidents fall under other categories such as health and safety and IT.

Clinical Incidents
A clinical incident is any unintended or unexpected incident which could have led to or did lead to harm for one or more patient’s receiving NHS care.

Corporate Business Incidents
A corporate business incident is a business event or circumstance that could have or did have a negative impact on the organisation, its stakeholders or the services in which it commissioned.

Cyber Incident
A Cyber-related incident is anything that could (or has) compromised information assets within Cyberspace. “Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services”. Source: UK Cyber Security Strategy, 2011.

Types of incidents could include:

- Denial of service attacks
- Phishing emails
- Social media disclosure

- Web site defacements
- Malicious Internal damage
- Spoof website
- Cyber bullying.

Fraud and Corruption
There are several specific offences under the Fraud Act 2006, however there are three primary ways in which it can be committed that are likely to be investigated by the Counter Fraud Specialist are:

- **Fraud by false representation** (section 2) – lying about something using any means
- **Fraud by failing to disclose information** (section 3) – not saying something when you have a legal duty to do so
- **Fraud by abuse of position** (section 4) – abusing your position of trust where there is a duty to safeguard financial interests of another person or organisation

An NHS insider may claim money for services not provided, claim more money than they are entitled to, or divert funds to themselves in other ways. External organisations may provide false or misleading information such as invoices, to claim money they are not entitled to.

If an incident relates to potential fraud, corruption or bribery, refer to the CCG Anti-Fraud, Bribery and Corruption Policy (CO06).

Harm
Harm is defined as an injury (physical or psychological), disease, suffering disability or death. In most circumstances harm can be considered to be unexpected, rather than the natural cause of the patients underlying condition.

Health and Safety, Fire, Environmental and Security Incidents
A health and safety, fire, environmental or security incident is an event or circumstance that affects staff/visitors safety.

Health and safety incidents will fall under one of the following categories:

- **Estates facilities** – for example a water leak, electricity outage, waste management or asbestos;
- **Fire** - an actual fire outbreak or false alarm;
- **Health and safety** – for example staff injury and accidents, moving and handling, hazardous substances, staff ill health (e.g. seizures or work related disorders);
- **Security** – for example damage/loss to organisation/personal property, loss of security badge/fob, or trespass

Information Governance (IG) Incidents
An information governance incident is an event or circumstance which affects or could affect the security of the information maintained by the CCG (including personal data).

IG incidents could include the following:

- Damage to hard copy records;
- Inappropriate access to/or disclosure of a person's information;
- Information left unattended (printer, empty office);
- Lost/stolen – equipment;
- Misdirected email containing confidential information;
- Misdirected hardcopy (e.g. post, fax etc.);
- Password sharing.

Information Technology (IT) Incidents

An information technology (IT) incident is an event or circumstance that affects or could affect the way the CCG does business negatively and is attributed to IT systems and/or the network. These incidents will most often include, but are not limited to:

- Hardware failure;
- Network failure;
- Software failure;
- Server failure;
- Telecommunications failure;
- Virus discovery.
- Cyber attack

National Reporting and Learning System (NRLS)

NRLS is a central database that captures all patient safety incidents (any unintended or unexpected incident that could have led or did lead to harm for one or more patients receiving NHS-funded healthcare).

All information submitted is analysed to identify hazards, risks and opportunities to continuously improve the safety of patient care.

Near Miss

An incident could be a **near miss** which is an event or situation that has the potential to cause harm but which never happened. These events should also be reported so the organisation can learn lessons and take preventative action where required.

North of England Commissioning Support Unit (NECS)

NECS is the Commissioning Support Unit (CSU) which provides incident support to the CCG.

NHS Commissioning Board / NHS England

The key functions and expertise for patient safety developed by the NPSA transferred to the NHS Commissioning Board Special Health Authority, known as NHS England, which subsequently merged with NHS Improvement.

Incidents reported on both the National Reporting and Learning System (NRLS) and Strategic Executive Information System (StEIS) are submitted to NHS England and Improvement.

Root Cause Analysis (RCA)
RCA is a systematic process whereby the factors that contributed to an incident are identified. As an investigation technique for incidents, it looks beyond the individuals concerned and seeks to understand the underlying causes and environmental context in which an incident happened.

Serious Incidents
For the full definitions of Serious Incidents see the **CCG CO18 Serious Incidents (SIs) Management Policy**. In summary these are incidents related to NHS-funded services and care resulting in:

- Unexpected or avoidable death;
- Unexpected or avoidable injury that has resulted in serious harm;
- Unexpected or avoidable injury that requires further treatment by a healthcare professional to prevent death of a service user, serious harm, actual or alleged abuse; sexual abuse, physical or psychological ill-treatment or acts of omissions which constitute neglect, exploitation, financial or material abuse, discriminative and organisational abuse, self-neglect, domestic abuse, human trafficking and modern day slavery;
- All Never Events;
- An incident (or series of incidents) that prevents, or threatens to prevent, an organisation’s ability to continue to deliver an acceptable quality of healthcare services; and
- Major loss of confidence in the service, including prolonged adverse media coverage or public concern about the quality of healthcare or an organisation.

Soft Intelligence
The phrase ‘soft intelligence’ is used to describe information gathered about a provider and its services, either from those who have experienced that service or from those with a professional relationship with the service. There may not be substantiated evidence to prove whether or not the event or experience occurred or has had an immediate measurable impact, but the intelligence may contribute to the bigger picture when looked at alongside hard intelligence and other evidence based information.

The Strategic Executive Information System (StEIS)
StEIS is a national database for reporting and learning from the most serious incidents in the NHS.

NECS Clinical Quality Team is responsible for recording serious incidents onto StEIS. This system is to be replaced by a new national consolidated system for reporting and leaning from serious incident in the near future.

3. Incident Reporting

All CCG Staff (permanent, fixed term and contractors) have a duty to report clinical and non-clinical incidents they are involved in, witness or have awareness of.

Specific employee responsibilities under this policy are described in section 6 of this document.

The reporting of incidents and near-misses is a key element in the governance of the organisation. Having a system that enables the capture and analysis of incident information is the cornerstone to effective risk management and can assist in the learning of lessons, prevention of harm and improvement of performance.

3.1 How to report a CCG incident

Employees and contractors who have access to the staff intranet have access to the electronic on-line incident reporting system SIRMS (Safeguard Incident and Risk Management System). SIRMS can be accessed at this web-address:

https://sirms.necsu.nhs.uk

Full guidance on how to report an incident via the web-from can be found in the CCG Incident Reporting and Management User Guide which can be on the staff intranet or GP Net.

If there are any difficulties accessing the web-form please contact a member of the NECS Governance team via: NECSU.SIRMSINCIDENTS@nhs.net

4. Management of CCG Incidents

The maintenance and administration of the incident reporting system 'SIRMS' is the responsibility of the NECS Governance Team. The operational management of specific incidents is the responsibility of the CCG:

- CCG Incident Manager
- Director of Nursing, Quality and Patient Safety
- CCG Governance Lead

The SIRMS incident reporting tool operates an email notification system whereby relevant persons are notified after the incident is reported by CCG staff. The notifications are as follows:

- Director of Quality and Patient Safety (and other relevant clinical/safeguarding roles) - clinical incidents;
- NECS Governance teams (e.g. Risk and Incidents, Health and Safety and Information Governance) are notified of relevant incidents; and
- CCG Governance Lead (non-clinical incidents).

It is the responsibility of the CCG to identify who is the most appropriate person to be the CCG Incident Manager (i.e. the person who follows-up the incident/email notification and completes the related management action form on SIRMS). This is usually the line manager of the incident reporter. This includes taking ownership of:

- Management of the incident;
- Management of risks associated with the incidents;
- Actions taken to mitigate further risks; and
- Implementation of action to address any lessons learned.

Full guidance on the management of incidents can be found in the CCG Incident Reporting and Management User Guide found on the CCG intranet.

4.1 Investigation of Incidents

Where incidents are sufficiently serious or complex, or part of an ongoing pattern, a formal investigation may need to take place to establish the root cause of the incident.

The degree of investigation is guided by the level of risk presented by the reported incident, which is measured by the Incident Assessment Matrix in Appendix 1. However it should be noted that as individual incidents can vary so too can the level of investigation required.

The standard approach to the investigation of any incident occurring within the organisation is to apply the principles of a Root Cause Analysis (RCA) to establish the true reasons for the incident so they may be prevented in the future. Further details how to perform Root Cause Analysis can be found in the Incident Reporting User Guide. The level of investigation required for clinical and non-clinical incidents differs. Full details can be found in section 4 and Appendix 2 for non-clinical incidents, and section 4.7 for clinical incidents.

In practical terms, any incident that takes place will usually generate a volume of paperwork related to its investigation and management. Full records must be retained of the investigation and outcomes (either attached to SIRMS or stored locally).

4.2 Interdependency of Incident and Risk Management

Management of incidents and risks through SIRMS is interdependent since risks can be identified through the monitoring of incident themes and trends. If a particular type of incident continues to occur, this is an indication that there is a risk that requires management through the SIRMS risk register.

Reasons for occurrence of an incident should be analysed and evidence established as to whether a trend of similar incidents exists, that need to be managed through the risk register. For further information refer to the CCG Risk Management Policy (CO14) and Risk Management procedure (SOP 16).

Both clinical and non-clinical incident reports are reviewed, as agreed, at the CCG's committees (as specified in section 5.1). This provides an opportunity for themes and trends to be picked up. These reports might indicate that there is a strategic risk e.g. if a number of practices are regularly reporting incidents around ambulance response times or referral problems. This is the most likely way that risks will be identified from incidents. It is unlikely that incidents reported by CCG staff will become a risk e.g. information governance or health & safety incidents, although not impossible.

4.3 Serious Incidents (SIs)

In some cases the outcome of an incident is such that it is immediately obvious that the incident is serious. In this instance the serious incident should be immediately reported to the Director of Nursing, Quality and Patient Safety.

The incident reporter uses the incident risk assessment matrix (Appendix 1) to assess the impact rating of the incident they are reporting. A consequence score of 5 (catastrophic) or 4 (high risk) indicates the incident is potentially serious and should be reported immediately to the reporter's Line Manager and Responsible Director.

If an incident is potentially serious the **CCG CO18 Serious Incidents (SIs) Management Policy should be invoked.** Advice on whether an incident meets the SI StEIS criteria can be sought from the CSU Clinical Quality Team for clinical issues or the CSU IG Team for Data Protection issues.

Although initial investigation and discussions may happen verbally a serious incident must be recorded on SIRMS as soon as possible and within 24 hours of identification.

See section 4.6 for potential serious incidents involving information governance /data protection.

The CSU Clinical Quality team is responsible for recording CCG serious incidents on to the Strategic Executive Information System (STEIS). Not all CCG serious incidents (e.g. an impact rating of 4 or 5) will be STEIS reportable. To ensure each potential serious incident is given due attention all CCG incidents scored 4 or 5 are sent (by the CSU Governance team for Risk and Incidents) to the CSU Clinical Quality Team for consideration (in conjunction with the CCG) to determine if the incident could be StEIS reportable~~.~~

4.4 Corporate Business Incidents

A corporate business incident is a business event or circumstance that could have or did have a negative impact on the organisation, its stakeholders or the services commissioned, or lead to financial loss.

The CCG, as commissioners, seek to assure that all services they commission or directly provide meet national identified standards. To ensure this is managed through their contracting process, compliance with serious incident (SI) reporting is a standard clause in all CCG contracts and service level agreements as part of the quality schedule.

A business incident that is reportable is likely to include one or more of the following:

- A lack of capacity or a service gap in meeting commissioning responsibilities
- A quality concern
- A communications breakdown.

For corporate (non-clinical) incidents the CCG Incident Manager determines for incidents scored 1 – 3 and near misses (scored 6) whether root cause analysis is required. This is influenced by any potential for the incident to re-occur, where there has been evidence of an emerging trend and the complexity of the incident. Root cause analysis must be performed for all incidents scored 4 and 5 (and the CSU Specialist Officer may request further input from the CCG as required).

For non-clinical incidents the level of investigation required, who leads the investigation, who is notified, and the incident closure timescales are summarised in Appendix 2.

An overview of CCG corporate business incident trends, themes and lessons learned will be reported to the CCG's Audit Committee through the Governance Assurance Report (GAR).

4.5 Health and Safety/Fire/Security/Environmental – RIDDOR Reportable Incidents

The organisation is statutorily obliged to report RIDDOR (Report of Injuries, Diseases and Dangerous Occurrences REGS, 1995) incidents to the Health and Safety Executive. There are various incidents which are RIDDOR reportable. Further information on RIDDOR categories can be obtained from the HSE website http://www.hse.gov.uk/riddor/reportable-incidents.htm.

The CSU Health and Safety Specialist will report the incident to the H&S Executive. If the incident recorded falls in to this category staff should email your CSU Health and Safety Specialist at: necsu.healthandsafety@nhs.net who can then advise accordingly.

The appointed CCG Incident Manager is responsible for managing updating and closing the CCG's Health & Safety incidents, on the SIRMS Incident Reporting and Management module.

4.6 Information Governance (IG) Incidents

The General Data Protection Regulation (GDPR)/Data Protection Act 2018 imposes legal obligations on data controllers to comply with the requirement to report specific breaches to the Information Commissioner's Office (ICO) without undue delay and no later than 72 hours of becoming aware of such a breach, where the breach is likely to result in a risk to the rights and freedoms of individuals.

It also requires that a data controller informs individuals affected by a breach of their personal data of the breach without undue delay, where the breach has or is likely to result in a risk to their rights and freedoms.

If a data processor suffers a breach, then under Article 33(2) it must inform the controller without undue delay as soon as it becomes aware. This allows the controller to take steps to address the breach and meet breach-reporting obligations under the GDPR. The requirements on breach reporting should be detailed in the contract between the controller and your processor, as required under Article 28. Processors are liable but only if it has failed to comply with GDPR provisions specifically relating to processors or it has acted without the controller's lawful instructions, or against those instructions.

There is no simple definition for a Data Security and Protection (DSP) reportable incident to the Information Commissioner What may at first appear to be of minor importance may, on further investigation, be found to be serious and vice versa. It is because of this that all /DSP incidents reported on SIRMS are quality checked daily by the CSU IG team. The CSU IG team checks the incident to assess if the incident needs to be reported to the Information Commissioner via the Data Security & Protection Toolkit (hosted by NHS Digital). The CSU DSP Officer will support the CCG in evidencing, collating and uploading a DSP reportable incident on the DSP Toolkit.

As a guide a DSP Reportable Incident (High Risk Incidents) could be any incident which involves actual or potential failure to meet the requirements of the Data Protection Act 2018 or General Data Protection Regulations) and/or the Common Law Duty of Confidentiality. This includes:

- 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; and
- Applies irrespective of the media involved and includes both electronic media and paper records.

The CSU IG Team reviews DSP incidents reported by the CCG and supports the management of DSP incidents where reportable to the ICO. The CSU will also provide updates and give advice for routine incidents where required. The appointed CCG Incident Manager manages updates and closes DSP reportable incidents on the Incident Reporting and Management Module of SIRMS, rather than the CSU IG team.

4.7 Clinical Quality Incidents

A clinical incident occurs when one or more patients are harmed or potentially harmed. It is expected that this type of incident will not often occur in a CCG organisation as there are limited clinical services provided. Staff should however use SIRMS to report clinical incidents they become aware of involving provider organisations (such as NHS Trusts, Care Homes etc.), or clinical incidents they witness or are involved in.

For clinical incidents who investigates the incident, the level of investigation required (including who performs it) and who manages the incident on SIRMS will depend on the nature and impact of the incident and the degree of harm (e.g. if a trend has emerged an investigation may be requested even if the incident reported is individually a low impact). The CSU Clinical Quality team will recommend the appropriate course of action. This could mean involving the CCG, GP Practice and Trusts in investigation and/or remedial action.

Clinical incidents generally fall into one of the following categories:

- ➢ Thematic Incidents – trends or themes across similar incident types
- ➢ Incidents Requiring an Individual Response.

The CSU Clinical Quality Team will update the SIRMS record showing the action taken (e.g. if the incident was referred to a provider for further investigation). Who provides further progress updates in SIRMS will depend on where the incident has been referred and whether the entity investigating and resolving the incident can access SIRMS. The CSU Clinical Quality Team will follow-up on incidents reported to external providers to ensure the incident is being satisfactorily managed.

The CCG or member practices are responsible for ensuring recommendations are satisfactorily implemented and the incident is fully resolved and closed on SIRMS.

The timescales for managing clinical incidents are as follows:

- **All** incidents will be reviewed by the Clinical Quality team within 5 working days;
- **Provider Investigated Incidents** – are submitted to providers requesting that they complete the investigation within one month.
- **StEIS Reportable Incidents** – Initial notification within 72 hours, then 60 working days to investigate and respond.

The CSU Clinical Quality team will consider in conjunction with the CCG if the incident falls into the category of a STEIS reportable Serious Incident and report accordingly in line with the CCG Serious Incidents (SIs) Management Policy (CO18). CCGs are required to report incidents that have a direct consequence on the safety of patients to the NRLS and this is managed by the CSU Clinical Quality team. The team is responsible for recording Serious Incidents on STEIS on behalf of the CCG.

4.8 Fraud and Corruption Incidents

Under no circumstances should suspicions of fraud, bribery or corruption be recorded as an incident in SIRMS. For details how to report these refer to the CCG's Anti-Fraud, Bribery and Corruption Policy (CO06) under the reporting section.

5. Trend Analysis / Learning Lessons

5.1 Internal Reporting of Incidents

SIRMS is capable of producing a range of reports based on the information fields and variables in the system. These reports can be tailored to the specific needs of the organisation via directorates, teams or committees. Reports can be used to feedback information on trends, learnt lessons and actions taken. Requests for specific tailored reports can be discussed with CSU Governance team.

An overview of corporate incidents reported across the organisation is provided to Audit Committee in the GAR report.

Clinical Quality/Patient Safety incidents are triaged on an individual basis and will be shared with the relevant provider/lead for investigation where appropriate. Incidents relating to primary care providers are also investigated and collated into themes. Clinical quality incident trends, themes and lessons learned are reported to the CCG's

Quality and Safety Group by the Clinical Quality team. The reports include incidents reported by GP practices about providers.

5.2 Levels of Investigation

It is the responsibility of the CCG to ensure that an appropriate investigation takes place following an incident or near miss according to the severity and possible implications of the incident. It is important to note that:

- All losses and compensations must be investigated
- All potential claims and complaints must be investigated

If the incident occurred within an external organisation (e.g. a provider of services), the incident must still be reported via SIRMS. The information reported as an external incident is useful for the CCG, as a commissioner and can be used to inform discussions in relation to provider service delivery and can be used as soft intelligence.

Incidents with an impact assessment of 1 to 3 may not require further action other than that specified in the initial incident form. Reassessment of any residual risk must be carried out after the implementation of any actions. For incidents with an impact assessment of 4 or 5, an investigation must always be carried out.

5.3 Onward Reporting

Occasionally, the CCG will be required to onward report trends and lessons learned for certain categories of incidents to other organisations. All serious incidents are initially reported through SIRMS. These incidents are then escalated via SIRMS to the appropriate team/contact person responsible for managing external reporting for:

NRLS	National reporting and learning system
STEIS	Strategic executive information system
DSP Toolkit	Data Security and Protection Reportable Incidents
RIDDOR	Report of injuries, diseases and dangerous occurrences regulations
HSE	Health and safety executive
ICO	Information Commissioners Office

6. Duties and Responsibilities

Membership	The membership has delegated responsibility to the Governing Body (GB) for setting the strategic context in which organisational process documents are developed, and for establishing a scheme of governance for the formal review and approval of such documents.
Governing Body	The Governing Body has delegated responsibilities from the CCG Members to ensure the CCG has appropriate arrangements to exercise its functions effectively and in accordance with good governance.
Clinical Management Board (CMB)	Clinical Management Board has responsibility for oversight of the CCG's arrangements for the discharge of its safeguarding duties, clinical governance and corporate governance, unless reserved to Governing Body, as reflected in the scheme of delegation. Specifically this includes: • Approving the Incident Reporting and Management Policy; • Ensure systems are in place and operating effectively for risk and incident management, information governance, health and safety and clinical risk; • Receive reports on incidents and serious incidents (including clinical, information governance and health and safety); and • Report any major or strategic issues to GB.
Quality and Safety Group	Quality and Safety Group has delegated oversight for the quality and safety of the CCG commissioning arrangements including receiving reports on clinical incidents and Serious Incidents. Concerns/issues are escalated to CMB as necessary.
Accountable Officer	The Accountable Officer has overall responsibility for the strategic direction and operational management, including ensuring that CCG process documents comply with all legal, statutory and good practice guidance requirements.
Director of Commissioning and Contracting	The Director of Commissioning and Contracting has overall responsibility for ensuring: • The incident management process is robust and adhered too • Incidents are maintained and managed in timely manner Staff have the necessary training required to implement the policy • Mechanisms are in place within the organisation for regular reporting and monitoring of incident themes and lesson learned
Responsible Directors	Directors are accountable to ensure any incidents within their remit of responsibility are managed to a satisfactory conclusion and lessons learned conducted and

	implemented (as required).
Managers	Managers have the responsibility: • Ensure the incident policy is followed within their area of responsibility; including managing incidents where they are the nominated CCG Incident Manager; • Support their staff with the reporting and management of incidents; and • Escalate incidents (where required) to their Responsible Director).
All Staff	All staff, including temporary and agency staff, are responsible for: • Compliance with relevant process documents. Failure to comply may result in disciplinary action being taken. • Co-operating with the development and implementation of policies and procedures and as part of their normal duties and responsibilities. • Identifying the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising their line manager accordingly. • Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager. • Attending training / awareness sessions when provided.
CSU (NECS) **Governance Department**	NECS Governance team will: • Provide incident management support and advice, including compliance with applicable laws and regulations; • Produce CCG incident reports as requested; • Identify trends, lesson learned and themes in incident reporting in order to identify any issues of concern for the CCG; • Provide training and assistance to the CCG in incident reporting and management in the SIRMS system; • Manage the administration of the SIRMS database; • Undertake an incident investigation in conjunction with CCG managers if required e.g. health and safety and IG incidents. • Report incidents as required to regulators (e.g. RIDDOR or ICO)
CSU (NECS) Clinical Quality Team	The NECS Clinical Quality team will: • Review clinical incidents to determine what action is required to manage the incident and communicate with the CCG, GP Practice or Trust (and other

	stakeholders where relevant) if further details are needed or actions are required; and • Determine for incidents relating to Primary Care or the CCG whether the incident meets the national guidance criteria as a Serious Incident and must be reported through StEIS and • Record Serious Incidents on StEIS.

7. Implementation

This policy will be available for all staff to use in the reporting and management of incidents and near misses.

All directors and managers are responsible for ensuring that relevant staff within their own directorates and departments have read and understood this document and are competent to carry out their duties in accordance with the procedures described.

The implementation of the detail of this policy is aligned into the full roll-out, development and implementation of the incident module of the SIRMS system across the CCG, their Member Practices and the CSU.

8. Training Implications

The sponsoring director will ensure that the necessary training or education needs and methods required to implement the policy or procedure(s) are identified and resourced or built into the delivery planning process. The training required to comply with this policy is:

Training	Staff Groups
General training	All staff
SIRMS incident reporting web-form for managers	Managers
Root Cause Analysis and incident investigation	Managers.

9. Fair Blame

The CCG is committed to a policy of ‘fair blame’. In particular formal disciplinary procedures will only be invoked following an incident where:

- There are repeat occurrences involving the same person where their actions are considered to contribute towards the incident;
- There has been a failure to report an incident in which a member of staff was either involved or about which they were aware (failure to comply with organisation’s policy and procedure);
- In line with the organisation and/or professional regulatory body, the action causing the incident is removed from acceptable practice or standards, or where;

- There is proven malice or intent.

Fair blame means that the organisation:

- Operates its incident reporting and management policy in a culture of openness and transparency which fulfils the requirements for integrated governance;
- Adopts a systematic approach to an incident when it is reported and does not rush to judge or apportion 'blame' without understanding the facts surrounding it; and
- Encourages incident reporting in the spirit of wanting to learn from things that go wrong and improve services as a result.

Further information in relation to a 'Just Culture' (aka fair blame) can be found at https://improvement.nhs.uk/resources/just-culture-guide/

9.1 Support for staff, and others

When an incident is reported it can be a stressful time for anyone involved, whether they are members of staff, a patient directly involved or a witness to the incident. They all need to know that they are going to be treated fairly and that lessons will be learned and action taken to prevent the incident happening again.

During an incident investigation, appropriate support will be offered to staff and anyone else involved in the incident if required. Support includes access to counselling services and the provision of regular updates of the investigation and its outcomes. Information is available on request from the Governance Team.

10. Documentation

10.1 Other Related Policy Documents

- CCG Risk Management Policy (CO14)
- CCG Anti-Fraud, Bribery and Corruption Policy (CO06)
- CCG Health & Safety policies and procedures (CO07)
- CCG Serious Incident Management policy (CO18)
- CCG Business Continuity Plan
- CCG Standards of Business Conduct and Declarations of Interest policy (CO19)
- Information Governance policies
- Complaints policy.

10.2 Legislation and Statutory Requirements

- The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (HMSO) 1995
- Serious Incident Framework 2018
- https://improvement.nhs.uk/documents/920/serious-incidnt-framwrk.pdf
- Revised Never Events Policy and Framework 2018

- https://improvement.nhs.uk/documents/2265/Revised Never Events policy and framework Final PDF
- Data Protection Act (2018)
- Working together to Safeguard Children, HM Government 2018
- No Secrets: Guidance on developing and implementing multi-agency policies and procedures to protect vulnerable adults from abuse (Department of Health 2000)
- NHS England Safeguarding Vulnerable People in the NHS: Accountability & Assurance Frameworks 2015
- NHS England Information Security Incident Reporting Procedure
- Guidance to the notification of Data Security and Protection Incidents 2018
- UK Cyber Security Strategy 2016 to 2021
- General Data Protection Regulations (GDPR)
- Freedom of Information Act 2000
- NHS England Risk Management Framework 2020
- NHS England Risk Management Manual 2020
- NHS Business Services Authority Whistleblowing Policy 2018
- Health and Social Care Act 2012.

11. Monitoring, Review and Archiving

11.1 Monitoring

The Clinical Management Board will agree a method for monitoring the dissemination and implementation of this policy. Monitoring information will be recorded in the policy database.

11.2 Review

The Clinical Management Board will ensure that this policy document is reviewed in accordance with the timescale specified at the time of approval. No policy or procedure will remain operational for a period exceeding three years without a review taking place.

Staff who become aware of any change which may affect a policy should advise their line manager as soon as possible. The Clinical Management Board will then consider the need to review the policy or procedure outside of the agreed timescale for revision

For ease of reference for reviewers or approval bodies, changes should be noted in the ‘document history’ table on the front page of this document.

NB: If the review consists of a change to an appendix or procedure document, approval may be given by the sponsor director and a revised document may be issued. Review to the main body of the policy must always follow the original approval process.

11.3 Archiving

The Clinical Management Board will ensure that archived copies of superseded policy documents are retained in accordance with Records Management: NHS Code of Practice 2016.

12. Equality Analysis

Initial Screening Assessment (STEP 1)

As a public body organisation we need to ensure that all our current and proposed strategies, policies, services and functions, have given proper consideration to equality, diversity and inclusion, do not aid barriers to access or generate discrimination against any protected groups under the Equality Act 2010 (Age, Disability, Gender Reassignment, Pregnancy and Maternity, Race, Religion/Belief, Sex, Sexual Orientation, Marriage and Civil Partnership).

This screening determines relevance for all new and revised strategies, policies, projects, service reviews and functions.

Completed at the earliest opportunity it will help to determine:

- The relevance of proposals and decisions to equality, diversity, cohesion and integration.
- Whether or not equality and diversity is being/has already been considered for due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED).
- Whether or not it is necessary to carry out a full Equality Impact Assessment.

Name(s) and role(s) of person completing this assessment:

Name: Elizabeth Durham.
Job Title: Senior Governance Officer.
Organisation: NECS

Title of the service/project or policy: Incident Management Policy

Is this a;
Strategy / Policy ✓ **Service Review** □ **Project** □
Other Click here to enter text.

What are the aim(s) and objectives of the service, project or policy:

This policy aims to set out the CCG's approach to the identification, reporting, investigation and management of incidents.

.

Who will the project/service /policy / decision impact?
(Consider the actual and potential impact)

- **Staff** ✓
- **Service User / Patients** □
- **Other Public Sector Organisations**□
- **Voluntary / Community groups / Trade Unions** □

- **Others, please specify** Click here to enter text.

Questions	Yes	No
Could there be an existing or potential negative impact on any of the protected characteristic groups?		✓
Has there been or likely to be any staff/patient/public concerns?		✓
Could this piece of work affect how our services, commissioning or procurement activities are organised, provided, located and by whom?		✓
Could this piece of work affect the workforce or employment practices?		✓
Does the piece of work involve or have a negative impact on: • Eliminating unlawful discrimination, victimisation and harassment • Advancing quality of opportunity • Fostering good relations between protected and non-protected groups in either the workforce or community		✓

If you have answered no to the above and conclude that there will not be a detrimental impact on any equality group caused by the proposed policy/project/service change, please state how you have reached that conclusion below:

Click here to enter text.

If you have answered yes to any of the above, please now complete the 'STEP 2 Equality Impact Assessment' document

Accessible Information Standard	Yes	No
Please acknowledge you have considered the requirements of the Accessible Information Standard when communicating with staff and patients. https://www.england.nhs.uk/wp-content/uploads/2017/10/accessible-info-standard-overview-2017-18.pdf	✓	
Please provide the following caveat at the start of any written documentation: **"If you require this document in an alternative format such as easy read, large text, braille or an alternative language please contact (ENTER CONTACT DETAILS HERE)"**		
If any of the above have not been implemented, please state the reason: Click here to enter text.		

Governance, ownership and approval

Please state here who has approved the actions and outcomes of the screening		
Name	**Job title**	**Date**
Richard Hay	Head of Planning and Operations	January 2021

Publishing

This screening document will act as evidence that due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED) has been given.

Appendix 1 - CCG Incident Assessment Matrix

Introduction

A risk-based approach is used to link incidents to the risk management framework.

The use of an incident grading system will help to assess the level of risk attributed to an incident, its seriousness and the level of investigation or analysis to be undertaken.

In some cases the outcome of the incident is such that it is immediately obvious that the incident is serious or significant.

When assessing the risk of an incident, reporters should use the assessment matrix outlined below.

Assessing the Incident

Determine the impact score (consequence) of your incident

From the submitted incident make a note of the cause group and choose the most appropriate domain from the left hand side of the table to assess the impact and determine the score. The number, on a scale of 1 to 5 is given at the top of the column. Note: the consequence will either be negligible, minor, moderate, major or catastrophic.

When scoring the consequence you are assessing either:

- The consequence of the incident that has occurred
- Or the likely consequence of a near miss should the incident have occurred

Incident Assessment Matrix

	Consequence score (severity levels) and examples of descriptors				
	1	**2**	**3**	**4**	**5**
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Impact on the safety of patients, staff or public (physical/psychological harm)	Minimal injury requiring no/minimal intervention or treatment. No time off work	Minor injury or illness, requiring minor intervention Requiring time off work for >3 days Increase in length of hospital stay by 1-3 days	Moderate injury requiring professional intervention Requiring time off work for 4-14 days Increase in length of hospital stay by 4-15 days RIDDOR/agency reportable incident An event which impacts on a small number of patients	Major injury leading to long-term incapacity/disability Requiring time off work for >14 days Increase in length of hospital stay by >15 days Mismanagement of patient care with long-term effects	Incident leading to death Multiple permanent injuries or irreversible health effects An event which impacts on a large number of patients
Quality/complaints/ audit	Peripheral element of treatment or service suboptimal Informal complaint/inquiry	Overall treatment or service suboptimal Formal complaint (stage 1) Local resolution Single failure to meet internal standards Minor implications for patient safety if unresolved Reduced performance rating if unresolved	Treatment or service has significantly reduced effectiveness Formal complaint (stage 2) complaint Local resolution (with potential to go to independent review) Repeated failure to meet internal standards Major patient safety implications if findings are not acted on	Non-compliance with national standards with significant risk to patients if unresolved Multiple complaints/ independent review Low performance rating Critical report	Totally unacceptable level or quality of treatment/service Gross failure of patient safety if findings not acted on Inquest/ombudsman inquiry Gross failure to meet national standards
Human resources/ organisational development/staffing/ competence	Short-term low staffing level that temporarily reduces service quality (< 1 day)	Low staffing level that reduces the service quality	Late delivery of key objective/ service due to lack of staff Unsafe staffing level or competence (>1 day) Low staff morale Poor staff attendance for mandatory/key training	Uncertain delivery of key objective/service due to lack of staff Unsafe staffing level or competence (>5 days) Loss of key staff Very low staff morale No staff attending mandatory/ key training	Non-delivery of key objective/service due to lack of staff Ongoing unsafe staffing levels or competence Loss of several key staff No staff attending mandatory training /key training on an ongoing basis
Statutory duty/ inspections	No or minimal impact or breech of guidance/ statutory duty	Breach of statutory legislation Reduced performance rating if unresolved	Single breach in statutory duty Challenging external recommendations/ improvement notice	Enforcement action Multiple breaches in statutory duty Improvement notices Low performance rating Critical report	Multiple breaches in statutory duty Prosecution Complete systems change required Zero performance rating Severely critical report

	Consequence score (severity levels) and examples of descriptors				
	1	**2**	**3**	**4**	**5**
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Adverse publicity/ reputation	Rumours Potential for public concern	Local media coverage – short-term reduction in public confidence Elements of public expectation not being met	Local media coverage – long-term reduction in public confidence	National media coverage with <3 days service well below reasonable public expectation	National media coverage with >3 days service well below reasonable public expectation. MP concerned (questions in the House) Total loss of public confidence
Business objectives/ projects	Insignificant cost increase/ schedule slippage	<5 per cent over project budget Schedule slippage	5–10 per cent over project budget Schedule slippage	Non-compliance with national 10–25 per cent over project budget Schedule slippage Key objectives not met	Incident leading >25 per cent over project budget Schedule slippage Key objectives not met
Finance including claims	Small loss Risk of claim remote	Loss of 0.1–0.25 per cent of budget Claim less than £10,000	Loss of 0.25–0.5 per cent of budget Claim(s) between £10,000 and £100,000	Uncertain delivery of key objective/Loss of 0.5–1.0 per cent of budget Claim(s) between £100,000 and £1 million Purchasers failing to pay on time	Non-delivery of key objective/ Loss of >1 per cent of budget Failure to meet specification/ slippage Loss of contract / payment by results Claim(s) >£1 million
Service/business interruption Environmental impact	Loss/interruption of >1 hour Minimal or no impact on the environment	Loss/interruption of >8 hours Minor impact on environment	Loss/interruption of >1 day Moderate impact on environment	Loss/interruption of >1 week Major impact on environment	Permanent loss of service or facility Catastrophic impact on environment

Appendix 2 – Process and Timescales for Managing and Closing Non-Clinical Incidents

Incident Severity		**Investigated by**	**Further Referrals and Notifications**	**Closed by**	**Root Cause Required?**	**Closure Timescale** (where possible)
1	Negligible/No Harm	CCG Incident Manager	CCG Governance Lead notified via SIRMS Notified to reporters line manager (the CCG Incident Investigating Manager unless agreed otherwise and responsible for completing the managers form).	CCG Incident Manager If the CSU Specialist requires further completion of actions they will review and complete the final closure.	Optional	5 working days
2	Low Risk					
3	Medium Risk					
4	High Risk	CCG Incident Manager (with support from the CSU Specialist) CCG Incident Manager to respond to the incident as soon as possible within 24 hours.	Immediate notification to the CCG Corporate Governance Lead and CSU Specialist Officer who will determine who else in the CCG / CSU should be involved. The CCG Corporate Governance Lead is notified via SIRMS. The incident will be notified to the reporter's line manager who will be the CCG Incident Manager (unless agreed otherwise).		Yes	1 month (If this target is not met an interim report must be submitted to the Corporate Governance Lead by the CCG Incident Manager).
5	Catastrophic					
6	Near Miss	CCG Incident Manager			Optional	5 working days
7	Soft Intelligence		N/A			