NHS
South Tyneside
Clinical Commissioning Group

Incident Reporting and Management Policy

Ratified	Audit and Risk Committee
Status	Final
Issued	February 2013
Approved By	Audit and Risk Committee
Consultation	Governance Team, NECS Clinical Quality Team, NECS Heads of Customer Programme, NECS Business Information Services, NECS South Tyneside CCG
Equality Impact Assessment	Completed
Distribution	All Staff
Date Amended following initial ratification	March 2019
Implementation Date	March 2019
Planned Review Date	March 2022
Version	V4.1
Author	Senior Governance Manager
Reference No	CO08

Policy Validity Statement
This policy is due for review on the 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 stynccg.enquiries@nhs.net

1. Version Control

Version	Release Date	Author	Update comments
V1	28/02/2013	Governance Lead, NHS South of Tyne and Wear	Policy provided to Clinical Commissioning Group (CCG) as part of policy suite
V2	10/03/2015	Julie Rutherford	Policy refresh in line with changing CCG incident reporting and management requirements aligned to the introduction of Safeguard Incident Risk System (SIRMS) across the CCG. Ratification DEFERRED pending further review and amendment.
V2.1	July 2015	Kate Watson	Updated in response to feedback from CCG Ex Committee March 2015. Table of contents updated. **Section 5** - updated types of incidents. Title of Section 8 amended and split into three separate sections. Glossary of terms now includes definition of 'contractors' and link to core set of never events. **Section 9.2** - amended as sentence repeated in 9.3. Appendices have been removed and **Section 10** now refers to a separate standard operating procedure to be used in conjunction with the policy. **Section numbers** changed to include new section at 10.2, Interdependency of incident and risk management. Section 10.3 has an additional sentence added. Section 10.7 has an additional sentence regarding clinical quality reporting. **Section 11.1** has information added regarding reporting mechanisms for clinical and non-clinical incident reports. **Section 12** – NECS roles and responsibilities updated to include customer relationship manager. **Section 14** – amended. **Section 16** – separated into four sections.
V3	23.02.16	Debra Elliott	Updated in line with national best practice guidance Policy updates **Section 8.3** Definitions - Glossary of Terms Serious Incident (SI) updated in line with NHSE SI policy guidance 2015 **Section 12** Duties & Responsibilities added in NECS Clinical Quality Manager will: Review clinical quality incidents reported by the CCG about providers that the CQ teams will manage these according to the processes agreed with CCGs and Providers **Section 16** References added in updated guidance - NHS England Serious Incident Framework 2015/16 and Never Event Framework 2015/16 Minor SOP updates in line policy changes outlined above
V4	26.10.18	Wendy Marley	Updated in line with GDPR, DPA 2018 and new reporting requirements for reportable data security and protection incidents **Section 8.3** Definition of NHS Digital added to reflect role in reportable IG incidents

			Section 8.3 Definition of serious incidents updated to include new requirements for reportable IG incidents. **Section 10.3** Investigation of Serious Incidents removes references to SIRI and refers instead to data breaches and reportable IT incidents. **Section 10.6** Updated in line with new requirements for reportable data security and protection incidents. **Section 16.3** Legislation and statutory requirements updated. **Section 17.3** Updated reference to Records Management code of practice. **Appendix 1** Updated Equality Impact Assessment
V4.1	January 2021	Wendy Marley	Updated for 12 months in light of COVID19

2. Approval

Role	Name	Date
Approval - deferred	Executive Committee	18/03/2015 (1)
Ratified	Executive Committee	30/07/2015 (2)
Ratified	Audit & Risk Committee	23/09/2015 (2)
Approved	Governing Body	26/11/2015 (2.1)
Approved	Audit & Risk Committee	08/03/2016 (3)
Approved	Audit & Risk Committee	March 2019 (4)
Approved	Virtual Executive Committee	April 2021 (4.1)

3. Review

This document will be reviewed twelve months from its issue date and every three years after its first review.

4. Table of Contents

5. 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 organisation 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 CCG employees (permanent, fixed term) and 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 reporting and 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 actions 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.

Incidents reported by the CCG will be predominantly non-clinical in nature therefore this policy focuses on the types of incidents that fall into this category.

The CCG uses Safeguard Incident and Risk Management System (SIRMS) as its incident reporting and management tool. SIRMS enables reporters to categorise incidents using a range of primary cause groups allowing incidents to be analysed to identify themes and trends.

The policy interlinks with the CCG's serious incident 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.

6. Status

This is a corporate policy and outlines the Incident Reporting and Management Policy for South Tyneside CCG.

7. 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:

- providing guidance on the process for reporting and managing incidents to CCG employees (permanent, fixed term) and contractors
- setting out the roles and responsibilities of CCG employees (permanent, fixed term) and 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, to ensure that no confusion exists between historical and current terms
- 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)
- integrating where relevant the existing organisational policy for Serious Incidents (SIs) **"CO18 CCG Serious Incidents (SIs) Management Policy";**
- providing a clear description of the reporting and management process based on the tools available in the Safeguard Incident Risk Management System (SIRMS), to ensure that all of the above can be achieved.

8. Definitions and Terms

The following definitions and terms are used in this policy document.

8.1 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:

- contractors
- employees
- environment (workplace)
- organisational reputation
- property
- service delivery
- stakeholder

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

- reputation
- resources
- staff
- quality of services

8.2 Examples of types of incidents

The following are examples of types of incidents used in this document:

Clinical Incident
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 Incident
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.

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

Information Governance Incident
An information governance incident is an event or circumstance which affects or could affect the security of the information maintained by the CCG.

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:

8.3 Glossary of Terms

The following terms are used in this document:

Contractors

In relation to this policy, 'contractors' refers to agency staff, and employees of NECS providing commissioning support services to the CCG. It does not include providers of clinical services. Contractors have a duty to report incidents they are involved in or witness in relation to the CCG.

Fraud, Corruption and Bribery

Fraud is essentially dishonest behaviour and is in very simple terms, "stealing".

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's Anti-Fraud Policy.

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 patient's underlying condition

National Reporting and Learning System (NRLS)

The NRLS is a central database of **patient safety incident reports**. Since the NRLS was set up in 2003, over four million incident reports have been submitted.

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.

NHS Digital (formerly Health and Social Care Information Centre)

NHS Digital has responsibility for standardising, collecting and publishing data and information from across the health and social care system in England. Health and social care organisations must use the Data Security and Protection Toolkit (DSPT) to provide assurance that they are practising good data security and that personal information is handled correctly. The DSPT is managed by NHS Digital.

NHS England

The key functions and expertise for patient safety developed by the National Patient Safety Authority (NPSA) **transferred to the NHS Commissioning Board Special Health Authority**, known as NHS England.

The Board Authority harnesses the power of the **National Reporting and Learning System (NRLS),** the world's most comprehensive database of patient safety information, to identify and tackle important patient safety issues at their root cause.

RCA (Root Cause Analysis)
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 (SI)
NHS England has produced an information resource to support the reporting and management of serious incidents which can be found in http://www.england.nhs.uk/wp-content/uploads/2015/04/serious-incidnt-framwrk-upd.pdf

Whilst the definition of a SI is quite broad, the following criteria outline the type of incidents which should be included:

1. Unexpected or avoidable death of one or more people. This includes:
   - Suicide/self-inflicted death
   - Homicide by a person in receipt of mental health care within the recent past

2. Unexpected or avoidable injury to one or more people that has resulted in serious harm.

3. Unexpected or avoidable injury to one or more people that requires further treatment by a healthcare professional in order to prevent:-
   - The death of the 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.

4. Never Events - all Never Events are defined as serious incidents although not all Never Events necessarily result in serious harm or death. Further information can be found at: http://www.england.nhs.uk/wp-content/uploads/2015/03/never-evnts-list-15-16.pdf

5. 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, including (but not limited to) the following:

   Failures in the security, integrity, accuracy or availability of information often described as data loss and/or information governance related issues (see Appendix 5 for further information);

   - Property damage

- Security breach/concern
- Incidents in population-wide healthcare activities such as screening or immunisation programmes where the potential for harm may extend to a large population;
- Inappropriate enforcement/care under the Mental Health Act (1983) and the Mental Capacity Act (2005) including Mental Capacity Act, Deprivation of Liberty Safeguards (MCA DOLS);
- Systematic failure to provide an acceptable standard of safe care (this may include incidents, or series of incidents, which necessitate ward/ unit closure or suspension of services); or
- Activation of Major Incident Plan (by provider, commissioner or relevant agency)

Where it is suspected that a reportable IG incident has taken place, it is good practice to informally notify key staff (Chief Executive, SIRO, Caldicott Guardian, other Directors etc.) as an "early warning" to ensure that they are in a position to respond to enquiries from third parties and to avoid 'surprises'. For cyber incidents notify the person responsible for any operational response (typically the Head of IT).

6. Major loss of confidence in the service, including prolonged adverse media coverage or public concern about the quality of healthcare or an organisation.

Reportable IG incident

Incidents falling into this category are essentially information governance or IT security related. These incidents must be reported to the Department of Health (DH) and the Information Commissioners Office (ICO) via NHS Digital's Data Security and Protection Toolkit. Both data controllers and data processors are responsible for reporting any personal data breach within 24 hours.

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 incidents in the near future.

9. Incident Reporting

Every CCG employee must ensure that any incident that they are involved in, witness or become aware of is reported either by themselves or another person. Specific employee duties and responsibilities under this policy are described in **section 12** 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.

9.1 How to report a CCG incident

CCG employees (permanent, fixed term) and contractors who have access to the staff intranet have access to the electronic on-line reporting system Safeguard Incident and Risk Management System (SIRMS). This is the preferred method for reporting incidents in the organisation. For the vast majority of staff, 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 **SIRMS incident web-form reporting guide** and the **SIRMS incident manager's web-form guide** (see Appendices 5 & 6 of the SOP).

If there are any difficulties accessing the web-form please contact a member of the NECS Governance team who will be pleased to help you. The Governance team can be contacted via email: NECSU.sirmsincidents@nhs.net

9.2 Where to record your incident in SIRMS:

CCG employees (permanent, fixed term) and contractors (with the exception of NECS staff) will report all CCG incidents they are involved in, witness or become aware of, on the **SIRMS CCG/GP incident reporting page**.

Contractors also have a responsibility to report incidents on their own incident reporting and management system as appropriate.

Should a NECS member of staff be involved in, witness or become aware of an incident the incident will be recorded on the **SIRMS NECS incident reporting page (NECS Staff)**. NECS have robust reporting mechanisms in place to ensure that, should the incident have a significant impact on the CCG, the relevant personnel in the CCG are informed, via established reporting mechanisms. E.g. if a NECS member of staff reported a commissioning or contracting incident via the NECS reporting page in SIRMS, the NECS Head of Customer Programme would be notified in order to facilitate discussion with the CCG where appropriate.

9.3 What to report

All CCG employees (permanent, fixed term) and contractors have a duty to report all incidents that they are directly involved in, have witnessed or have an awareness of. This can mean the reporting of incidents most commonly associated with incident reporting such as slips, trips/ falls, road traffic accidents or information governance breaches, corporate business incidents and IT.

10. Management of CCG Incidents

The maintenance and administration of the incident reporting system is largely the responsibility of the Governance Team within NECS Organisational Development and Corporate Services Directorate. The operational management of specific incidents is the responsibility of the CCG:

- CCG Director of Operations
- CCG Incident Investigating Manager

The SIRMS incident reporting tool operates an email notification system within which the CCG Director of Operations is informed of the incident when submitted by CCG staff.

It is the responsibility of the CCG Director of Operations to identify who is the most appropriate person to follow up the incident/email notification and fill in the related management action form which ensures ownership of:

- the management of the incident
- the management of risks associated with the incidents
- the action taken to mitigate further risk
- the implementation of action to address any lessons learned

A standard operating procedure (SOP) has been developed to support the reporting and management of incidents, which outlines the process that reporters and managers should follow, and consists of the following documents:

- **Appendix 1** – Incident Management Process: Non-clinical Incidents (Corporate Business / Health and Safety / Information Governance and IT Incidents)
- **Appendix 2** – Incident Management Process: Clinical Quality Incidents
- **Appendix 3** – Incident Assessment Matrix
- **Appendix 4** – Incident Reporters Frequently Asked Questions
- **Appendix 5** – SIRMS Incident Web-form Reporting Guide
- **Appendix 6** – Incident Manager's Checklist
- **Appendix 7** – SIRMS Incident Managers Web-form guide
- **Appendix 8** – Root Cause Analysis Guide

The SOP should be used in conjunction with this policy.

10.1 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 level of investigation, guided by the level of risk presented by the reported incident, should be measured as part of the reporting procedure by both the reporter and the Incident Investigating Manager. 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. Refer to the RCA guidance in Appendix 8 of the SOP.

In practical terms, any incident that takes place will usually generate a volume of paperwork related to its investigation and management. The SIRMS enables users to attach electronic documents to the individual incident files. Once incidents are reported onto the SIRMS, managers are encouraged to use the system as an archive for key documents and information related to the incident, for example, investigation reports, meeting notes or risk assessments.

10.2 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 Section 7.7.2, Risk Materialisation, in the CCG's Risk Management Policy.

Both clinical and non-clinical incident reports are reviewed, as agreed, at the CCG's committees (as specified in section 11.1). This provides an opportunity for themes are 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.

10.3 Investigation of 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 CCG Director of Operations. To help you assess the risk score of a CCG incident, the reporter should use the incident assessment matrix, (see Appendix 3 of SOP). The matrix demonstrates the criteria for scoring the consequence of the incident (which indicates the seriousness of the incident).

A consequence score of 5 (catastrophic) or 4 (high) indicates the incident is serious and this should be reported immediately to the CCG Director of Operations.

A management response is required as soon as possible within a 24 hour period. These incidents need to be reported verbally if possible and recorded immediately on SIRMS (within a 24 hour period).

NECS Clinical Quality Team is responsible for recording CCG serious incidents on to the Strategic Executive Information System (StEIS). Not all CCG serious incidents will be StEIS reportable, but to ensure each serious incident is given due attention, SIRMS will immediately trigger all CCG reported serious incidents to the Clinical Quality Team's generic mailbox for consideration.

Incidents involving the use of 'Personal Confidential Data' or IT incidents that have significant impact on the delivery of essential services may be recorded on StEIS as well as through the Data Security and Protection Toolkit.

10.4 Corporate Business Serious Incidents

The CCG, as commissioners, seek to assure that all services they commission or directly provide meet national identified standards, and to ensure that 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.

The impact of a business incident is likely to have led to a financial loss or a negative impact on the reputation of the business.

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

An overview of CCG corporate business incident trends, themes and lessons learned will be reported to the CCG's:

- Audit and Risk Committee
- Governing Body

Refer to Appendix 1 of the SOP.

10.5 Health and Safety/Fire/Security/Environmental, Serious Incidents - RIDDOR Reportable

The organisation is statutorily obliged to report RIDDOR (Report of Injuries, Diseases and Dangerous Occurrences REGS**,** 1995) incidents to the Health and Safety Executive (HSE). Incidents must be reported to RIDDOR when someone has been absent from work for more than 7 days due to an incident. Your NECS Health and Safety Governance Specialist will report the incident to the HSE on your behalf. If the incident recorded falls into this category, staff should email NECS Health and Safety Governance Specialist at: necsu.healthandsafety@nhs.net and advise accordingly.

Refer to Appendix 1 of the SOP.

10.6 Information Governance (IG) and Information Technology (IT) Serious Incidents

The General Data Protection Regulations (GDPR)/UK Data Protection Act 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 when it is likely to result in a high risk to the rights and freedoms of individuals.

GDPR/UK Data Protection Act requires that a controller informs individual affected by a breach of their personal data of the breach without undue delay, where the breach is likely to result in a risk to the rights and freedoms of individuals.

NHS Digital's guidance 'Guide to the Notification of
Data Security and Protection Incidents' sets out three main types of personal data breach:

- Confidentiality breach- unauthorised or accidental disclosure of, or access to personal data
- Availability breach- unauthorised or accidental loss of access to, or destruction of, personal data
- Integrity breach - unauthorised or accidental alteration of personal data

The IG team will impact check daily CCG incidents recorded in SIRMS to determine if the recorded incident is reportable to NHS Digital Data Security Centre and the Information Commissioner's Office through the Data Security and ProtectionToolkit. The NECS IG Team will assist the CCG in making this assessment and reporting appropriately. Where it is suspected that a reportable data security and protection incident has taken place, it is good practice to informally notify key staff (Chief Officer, SIRO, Caldicott Guardian, other directors etc.) as an 'early warning' to ensure that they are in a position to respond to enquiries from third parties and to avoid 'surprises'.

Article 34 of GDPR requires any personal data breach that is likely to result in a high risk to the rights and freedoms of individuals, to be communicated with those affected.

Any communication must contain the following four elements

- description of the nature of the breach;
- name and contact details of the data protection officer or other contact point from whom more information can be obtained;
- description of the likely consequences of the personal data breach;
- description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

A communication is not necessary in the following three circumstances:

- The controller has implemented appropriate technological and organisational protection measures which were applied to the personal data affected by the breach for example the data were encrypted.
- The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms if individuals is no longer likely to materialise.
- It would involve a disproportionate effort. However, there is still an obligation to have a communication by another means such as a press notice or statement on the organisation website.

If an organisation decides not to notify individuals, it will still need to notify the ICO unless it can demonstrate that the breach is unlikely to result in a risk to rights and freedoms.

Refer to Appendix 1 of the SOP.

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

IT events that have a significant impact on the continuity of essential services should be reported immediately to the NECS IT service desk and the CCG’s IT lead should be informed. NECS Business Information Services will assess these incidents to determine whether they need to be reported in line with Network and Information Systems Regulations (NIS).

These incidents might involve GP network issues or problems with telephony in practices.

Types of incidents could include:

- Denial of service attacks
- Phishing emails
- Social media disclosures
- Web site defacement
- Malicious internal damage
- Spoof website
- Cyber bullying

Refer to Appendix 1 of the SOP.

10.7 Clinical Quality Serious Incidents

A Clinical quality Incident occurs when one of more patients is harmed or potentially harmed. It is expected that this type of incident will not often occur in a CCG organisation as they do not provide clinical services. CCG employees (permanent, fixed term) and contractors, have a duty to report any clinical quality incidents they witness, are involved in or become aware of. To report these, staff are instructed to use the CCG/GP reporting an incident page of SIRMS - https://sirms.necsu.nhs.uk/

The NECS clinical quality team leads in the management of patient safety clinical incidents in CCGs and GP member practices. The team is responsible for recording serious incidents on StEIS. Not all serious incidents will be StEIS reportable, but to ensure each serious incident is given due attention, SIRMS automatically triggers all CCG reported serious incidents to the Clinical Quality team's generic mailbox.

The clinical quality team will consider if the serious incident falls into the category of a StEIS reportable SI and report accordingly using guidance found in 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 (National Reporting and Learning System); this is a clinical quality team function.

SIRMS is configured to escalate incidents to the clinical quality team in line with the SI policy.

Clinical quality incident trends, themes and lessons learned are reported to the CCG's Quality and Patient Safety Committee by the clinical quality team. Reports feature incidents recorded by GP practices about providers.

Refer to Appendix 2 of the SOP.

10.8 Fraud and Corruption Serious incidents

All cases of suspected fraud or corruption should be notified immediately to the Chief Finance Officer who will then give advice or arrange investigation of the incident, in accordance with the CCG Standing Financial Instructions.

Sunderland Internal Audit Services (SIAS) is commissioned to support the CCG with their counter- fraud arrangements through their Internal Audit Function.

11. Trend Analysis / Learning Lessons

11.1 Internal Reporting of Incidents

SIRMS is capable of producing a range of reports based on all of the information fields and variables on the SIRMS incident reporting/management system at regular intervals. These reports can be tailored to the specific needs of the organisation via directorates, teams or committees. They can be used to feedback information on trends, lessons learned and actions taken. Requests for specific tailored reports can be made to NECS Governance Team - NECSU.sirmsincidents@nhs.net

An overview of incidents reported across the organisation will be monitored for trends, themes and lessons learned through a number of committees, which include:

- Quality, Patient Safety and Risk Committee – who will receive reports from the Clinical Quality team on GP reported incidents regarding providers.
- Audit and Risk Committee – who will receive a summary of CCG reported non-clinical incidents via the quarterly Governance and Assurance Report as identified in the committee's cycle of business.
- Governing Body - who will receive a summary of CCG reported non-clinical incidents via the quarterly Governance and Assurance Report as identified in the committee's cycle of business.

The Director of Operations and Operations and Operations Manager will also receive an incident report at the beginning of each month.

11.2 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 a different organisation, the incident must still be reported for appropriate investigation and a decision made as to the most appropriate lead for the investigation.

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.

11.3 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
- SIRI – Serious incidents requiring investigation
- RIDDOR - Report of injuries, diseases and dangerous occurrences regulations The health and safety executive
- The information commissioner's office
- NHS Protect – protection against fraud and corruption in the NHS.

Requests for specific tailored reports will be agreed with NECS and CCG. NECSU.sirmsincidents@nhs.net

12. Duties and Responsibilities

Council of Practices	Have 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.
Chief Officer	The Chief 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 Operations (CCG Information Governance Lead)	The Director of Operations has overall responsibility for ensuring: • The incident management process is robust and adhered to. • 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. • Confirm to NECS Senior Governance Officer that incidents can be marked as fully completed.
Line Managers	The service leads have the responsibility: • To support their directors and staff to maintain the incident policy and to manage individual incidents in accordance with policy. • To work closely with the Director of Operations to ensure a transparent and consistent approach to incident management across the CCG in partnership with key stakeholders. All line managers and supervisory staff are responsible for the adherence and monitoring compliance within this policy.
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 as part of their normal duties and responsibilities. • Identify the need for a change in policy or procedure as a result of becoming aware of changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising there line manager. • Attending training/awareness sessions when provided.

North of England commissioning (NECS)	NECS senior governance officer will: • Provide incident management support and advice. • Produce CCG reported incident reports as requested. • Identify trends, lessons 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. NECS clinical quality manager will: • Consider if a serious incident falls into the category of a StEIS reportable SI and report accordingly. • Review clinical quality incidents reported by the CCG. • Review clinical quality incidents reported by the CCG about providers that the CQ teams will manage these according to the processes agreed with CCGs and Providers • Provide clinical quality incident reports as requested. Customer relationship manager: • Receive notification of incidents relating to CCG reported corporate business incidents. • Facilitate discussion with the CCG regarding corporate business incidents, where appropriate.
NECS Information Governance Lead	NECS information governance lead has the responsibility to: • Provide information governance support to staff in the organisation. • Co-ordinate different areas of information governance and to ensure progress against key standards and requirements. • In collaboration with IT, develop, implement and monitor information security across the organisation. • Support the CCG in evidence collation, upload and publicise the IG Toolkit.

13. Implementation

13.1 This policy will be available to all Staff for use in the circumstances described on the title page.

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

13.3 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 across the CCG, NECS and their Council Members.

13.4 This policy is reviewed at regular intervals to ensure that the implementation of the processes contained in the policy are in line with the practical experience of users of the SIRMS.

14. Training Implications

The sponsoring director will ensure that the necessary training or education needs and methods required to implement the policy are identified and resourced or built into the delivery planning process. This may include identification of external training providers or development of an internal training process.

The level of training required in incident reporting and management varies depending on the level and responsibility of the individual employee.

The training required to comply with this policy is key to the successful implementation of the policy and embedding a culture of incident reporting and management in the organisation. Through a training and education programme, staff will have the opportunity to develop more detailed knowledge and appreciation of the role of incident reporting and management. Training and education will be offered through a rolling programme of incident reporting and management training.

15. 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 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 'blame' without understanding the facts surrounding it
- encourages incident reporting in the spirit of wanting to learn from things that go wrong and improve services as a result.

15.1 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.

16. Documentation

16.1 Other Related Documents

- Security Procedure
- First Aid Procedure
- Fire Safety Procedure
- Business Continuity Plan

16.2 CCG policies

- HR35 Whistleblowing Policy
- IG01 Confidentiality and Data Protection Policy
- IG02 Data Quality Policy
- IG03 Information Governance and Information Risk Policy
- IG04 Information Access Policy
- IG05 Information Security Policy
- IG06 Records Management Policy and Strategy
- CO02 Complaints Policy and Procedure
- CO05 Fire Safety Policy
- CO06 Anti-Fraud Policy
- CO07 Health and Safety Policy
- CO11 Moving and Handling Policy
- CO14 Risk Management Policy
- CO17 Security Policy
- CO18 Serious Incidents (SIs) Management Policy
- CO20 Violence, Aggression and Abuse Management Policy

16.3 Legislation and statutory requirements

- NHS Digital Guide to the notification of data security and protection incidents July 2018
- Data Protection Act 2018
- NHS England Incident reporting policy October 2012
- No secrets: Guidance on developing and implementing multi-agency policies and procedures to protect vulnerable adults from abuse (Department of Health) 2000
- NHS England Serious Incident Framework 2015/16 and Never Event Framework 2015/16
- The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (HMSO) 1995
- Working together to safeguard children, (HM Government) 2006
- UK Cyber Security Strategy, 2011

16.4 References

The major references consulted in preparing this policy are described above.

17. Monitoring, Review and Archiving

17.1 Monitoring

The Director of Operations will oversee, on behalf of the executive committee, a method for monitoring the dissemination and implementation of this policy.

17.2 Review

The Director of Operations will ensure that each 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 changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives that affect, or could potentially affect policy documents, should advise the Director of Operations as soon as possible, via line management arrangements. The Director of Operations 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.

17.3 Archiving

The Director of Operations will ensure that archived copies of superseded policy documents are retained in accordance with Records Management: Code of Practice for Health and Social Care 2016

Appendix 1 Equality Analysis

North of England Commissioning Support

Partners in improving local health

An Equality Impact Assessment (EIA) is a process of analysing a new or existing service, policy or process. The aim is to identify what is the (likely) effect of implementation for different groups within the community (including patients, public and staff).

We need to:

- Eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Equality Act 2010
- Advance equality of opportunity between people who share a protected characteristic and those who do not
- Foster good relations between people who share a protected characteristic and those who do not

This is the law. In simple terms it means thinking about how some people might be excluded from what we are offering.

The way in which we organise things, or the assumptions we make, may mean that they cannot join in or if they do, it will not really work for them.

It's good practice to think of all reasons why people may be excluded, not just the ones covered by the law. Think about people who may be suffering from socio-economic deprivation or the challenges facing carers for example.

This will not only ensure legal compliance, but also help to ensure that services best support the healthcare needs of the local population.

Think of it as simply providing great customer service to everyone.

As a manager or someone who is involved in a service, policy, or process development, you are required to complete an Equality Impact Assessment using this toolkit.

Policy	A written statement of intent describing the broad approach or course of action the Trust is taking with a particular service or issue.
Service	A system or organisation that provides for a public need.
Process	Any of a group of related actions contributing to a larger action.

STEP 1 - EVIDENCE GATHERING

Name of person completing EIA:	**Senior Governance Officer, NECS**
Title of service/policy/process:	**CO08: Incident Reporting and Management Policy**
Existing: ☑ New/proposed: ☐ Changed: ☐	
What are the intended outcomes of this policy/service/process? Include outline of objectives and aims	
This policy aims to set out the CCG's approach to incident reporting and the management of incidents in fulfilment of its overall objective to commission high quality and safe services. In addition, the adoption and embedding within the organisation of an effective incident reporting and management policy and processes will ensure that the reputation of the CCG is maintained and enhanced, and its resources are used effectively to reform services through innovation, large- scale prevention, improved quality and greater productivity.	
Who will be affected by this policy/service /process? (please tick)	
☑ Staff members	
☑ Other	
If other please state:	
Patients, Staff from other organisations, Public.	
What is your source of feedback/existing evidence? (please tick)	
☐ National Reports ☑ Staff Profiles	
☐ Staff Surveys ☑ Complaints/Incidents	

☐ **Focus Groups** ☑ **Previous EIAs** ☑ **Other**	
If other please state: • **Feedback from committee meetings where incidents are discussed** • **Staff who contact the NECS governance service for help and assistance where required**	

Evidence	**What does it tell me? (About the existing policy/process? Is there anything suggest there may be challenges when designing something new?)**
National Reports	**NA**
Staff Profiles	**NA**
Staff Surveys	**NA**
Complaints and Incidents	**Buy in from reporters and managers**
Staff focus groups	**NA**
Previous EIAs	**NA**
Other evidence (please describe)	**NA**

STEP 6- ACTION PLAN

Ref no.	**Potential Challenge/** **Negative Impact**	**Protected Group Impacted (Age, Race etc)**	**Action(s) required**	**Expected Outcome**	**Owner**	**Timescale/** **Completion date**
NA		All	**Ongoing incident reporting and management support to staff.**	Positive - increased by in and awareness of process	**WM**	**Ongoing**

Ref no.	**Who have you consulted with for a solution? (users, other services, etc)**	**Person/** **People to inform**	**How will you monitor and review whether the action is effective?**
NA	SIRMS users / Committee Members	CCG Operations Manager.	Evaluation of training

 **SIGN OFF**

Completed by:	**Helen Ruffell**
Signed:	
Presented to: (appropriate committee)	**Audit and Risk Committee**
Publication date:	**March 2019**