NHS
County Durham
Clinical Commissioning Group

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

Version Number	**Date Issued**	**Review Date**
V2	December 2020	December 2022

Prepared By:	Senior Governance Officer North of England Commissioning Support
Consultation Process:	Director of Nursing Head of Governance NECS Senior Manager Clinical Quality NECS Senior Governance Officer NECS Governance & Assurance Manager
Formally Approved:	8th December 2020
Approved By:	Executive Committee
Policy Adopted From:	CO08 Incident Reporting and Management Policy (1)

Equality Impact Assessment

Date	**Issues**
October 2020	See Section 11

Accessibility Information Standard

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

POLICY VALIDITY STATEMENT

Policy users should ensure that they are consulting the currently valid version of the documentation. The policy will remain valid, including during its period of review. However, the policy must be reviewed at least once in every 3 year period.

Version Control

Version	Release Date	Author	Update comments
V1	April 2020	Governance & Assurance Manager & Senior Governance Officer North of England Commissioning Support	New policy template.
V2	December 2020	Senior Governance Officer North of England Commissioning Support	Policy refresh to update: • Data Security and Protection guidance update • Health and Safety CCG process update • SIRMS process updates • New equality impact assessment and template • Fraud and corruption incident guidance updates • CSU Clinical Quality Process updates • NHS policy, legislation and statutory requirements • Appendix 2 Glossary of terms update • Appendix 3 CCG Matrix update

Approval

Role	Name	Date
Approval (1)	Combined Management Group	10 March 2020
Approval (2)	Executive Committee	8 December 2020

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, the 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 are 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 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 CCG incident reporting and management policy covers the following broad categories:

- Corporate business incident
- Fraud and corruption
- Health and safety/ fire/ security or environmental incidents
- Information governance / Data Security & Protection (DSP) Incidents
- I.T (information technology) and cyber security incidents
- Clinical incidents.

The policy framework interlinks with CCG CO18 Serious Incidents (SIs) Management Policy for the reporting and management of serious incidents and the CCG’s Business Continuity Plan.

The adoption and embedding of an effective integrated incident management framework within the organisation 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.

1.2 Purpose and Scope

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

This policy outlines the Incident Reporting and Management framework to CCG staff. The Framework will be achieved by:

- Providing guidance on the process for reporting and managing incidents to CCG employees and contractors (supported by the SIRMS CCG Incident Reporting and Management User Guides)
- 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 definitions of the types of incidents that can be reported within the organisation's incident reporting system
- Providing clear principles of incident investigation (when responding to incidents, including fair blame and root cause analysis)
- Outlining how actions, outcomes, trends and lessons learned from incidents are monitored and reviewed
- Outlining 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) CCG CO18 Serious Incidents (SIs) Management Policy and the CCG's Business Continuity Plan.

2. Definitions

The following definitions and terms are referenced throughout this document.

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 learning 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 and Contractors
- Quality of services the CCG provides and commissions.

It is important to note that:

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

2.2 Glossary of Terms

A Glossary of Terms can be located at Appendix 2

3. Incident Reporting

All CCG staff (permanent, fixed term and contractors) 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 responsibilities under this policy are described in Appendix1 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 incident & risk management and can assist in the learning of lessons, prevention of harm and improvement of performance.

3.1 How and Where to report a CCG incident

All CCG employees (permanent, fixed term etc.) and contractors have a duty to report all clinical and non-clinical incidents they are involved in, witness or have an awareness of. All CCG employees and contractors have access to the CCG electronic on-line reporting system - Safeguard Incident and Risk Management System, (SIRMS). 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-form can be found in the SIRMS CCG incident management user guide.

If there are any difficulties accessing the web-form or user guide please contact a member of the SIRMS team. The CSU SIRMS team can be contacted via email: NECSU.SIRMSINCIDENTS@nhs.net

4. Management of CCG Incidents

The maintenance and the administration of SIRMS is largely the responsibility of the CSU Governance team. The operational management of specific incidents is the responsibility of the CCG. Specific duties are outlined in the duties and responsibilities section of this policy.

The SIRMS incident reporting tool operates an email notification system. The CCG Corporate Investigating Manager is notified directly from the system when an incident related or involving the CCG has been reported.

It is the responsibility of the CCG Corporate Investigating Manager to identify who is the most appropriate person to action the incident and complete the related management action form which ensures ownership of the:

- Management of the incident
- Management of risks associated with the incident
- Action taken to mitigate further risk
- Implementation of action to address any lessons learned.

Further information on the management of routine incidents can be obtained from the SIRMS CCG Incident Reporting and Management User Guide.

4.1 Investigation of Routine incidents

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. The SIRMS CCG Incident Reporting and Management User Guide provides further information and guidance on RCA principles.

The incident investigating manager and reporter should assess the risk of the incident as part of the reporting process. The level of risk should be apportioned to the type of incident.

SIRMS enables users to attach electronic documents to the individual incident files. Once incidents are reported onto 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.

4.2 Investigation of Serious Incidents (SIs)

Where incidents are sufficiently serious or complex, or part of an ongoing pattern, a formal investigation to establish the root cause of the incidents required. An incident impact score of 5 (catastrophic) or 4 (high risk) indicates the incident is serious and should be reported immediately to the Chief Officer and the CCG Head of Corporate Services, who will appoint the Investigating Officer to carry out an RCA. All incidents reported should be discussed with the reporter’s Line Manager.

The incident reporter uses the incident risk assessment matrix (appendix 3) to assess the impact rating of the incident they are reporting.

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

Where it is suspected that a Data Security and Protection reportable incident (high risk incidents) has taken place, it is good practice to informally notify key staff (Accountable Officers, SIRO, Caldecott Guardian, other Directors and Data Protection Officer etc.) as an “early warning” to ensure that they are in a position to respond to enquiries from third parties and to avoid ‘surprises’.

The General Data Protection Regulation (GDPR)/UK Data Protection Bill imposes legal obligations on 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 (see section 4.3). For cyber incidents notify the person responsible for any operational response. Section 4.3 outlines further information on Data Security and Protection reportable incidents.

An incident involving the use of “Personal Confidential Data” is defined as an incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals. This should be considered as serious.

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 will be STEIS reportable.
To ensure each serious incident is given due attention all CCG serious incidents will be sent by the CSU Governance team to the CSU Clinical Quality Team for consideration in conjunction with the CCG to determine if the incident could be StEIS reportable.

4.3 Information Governance (IG) / Data Security and Protection Reportable Incidents (High Risk Incidents) and Information technology (IT) Serious Incidents

The General Data Protection Regulation (GDPR)/UK Data Protection Bill imposes legal obligations on 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.

GDPR/UK Data Protection Bill requires that a controller informs individuals affected by a breach of their personal data 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
- 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 Corporate Investigating Manager manages updates and closes DSP reportable incidents on the Incident Reporting and Management Module of SIRMS, rather than the CSU IG team.

4.4 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. 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 and advise accordingly.

The appointed CCG Investigating Officer is responsible for managing updating and closing the CCG's Health & Safety incident, on the SIRMS Incident Reporting and Management Module.

4.5 Patient Safety Clinical 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. However, staff should use SIRMS to report clinical incidents they become aware of involving provider organisations (such as NHS Trusts, Care Homes etc.) This would include an instance where a Regulation 28 (preventing future deaths) is received. These are received very rarely and once reported on SIRMS, the CCG would be responsible for any further action via the CCG Quality Committee.
Staff (permanent, fixed term and contractors), have a duty to report any clinical incidents that they witness or are involved in. To report these, staff are instructed to use the CCG/GP reporting incident page of SIRMS - https://sirms.necsu.nhs.uk/

The CSU Clinical Quality team leads in the management of patient safety clinical incidents in CCGs and GP member practices. The CSU Clinical Quality team is notified of all patient safety clinical incidents reported on SIRMS. The team is responsible for recording serious incidents on STEIS on behalf of the CCG.

The CSU Clinical Quality team will consider in conjunction with the CCG if the serious incident falls into the category of a STEIS reportable Serious Incident and report accordingly in line with the CCG Serious Incidents (SIs) Management Policy. CCGs are required to report incidents that have a direct consequence on the safety of patients to the NRLS, this is managed within the CSU Clinical Quality team. Advice on whether an incident meets the SI StEIS criteria can be sought from NECS Clinical Quality Team for clinical issues or NECS IG Team for Data Protection issues.

4.6 Corporate Business Serious Incidents

A corporate business incident is an event or circumstance that could have or did have a negative impact on the way the CCG conducts business with their stakeholders and/ or that could lead to financial loss. Corporate business incidents events or consequences may also be included in the CCG's risk register.

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 might 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.

4.7 Fraud and Corruption Serious Incidents

If there is a suspicion of theft, fraud, or other untoward events taking place at work staff should:

- Make a note of their concerns
- In the case of theft contact the Local Security Management Specialist
- In the case of fraud contact the Local Counter Fraud Specialist
- You can also report to the national NHS Fraud and Corruption Reporting Line on 0800 028 40 60 or www.reportnhsfraud.nhs.uk/

Staff should not be afraid of raising concerns and will not experience any blame or recrimination as a result of making any reasonably held suspicion known.

If staff have any concerns about any of the issues raised in this document, they should contact their manager or "Human Resources Manager".

The CCG's Anti-Fraud, Bribery and Corruption Policy outlines the CCG's responsibilities in delivering a comprehensive approach to ensure that all suspected economic crime is referred appropriately.

5. Trend Analysis/Learning Lessons

5.1 Internal reporting of Incidents

SIRMS is capable of producing a range of reports based on all of 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 will be monitored for trends, themes and lessons learnt on a quarterly basis and discussed at the relevant CCG Committee. Clinical Quality/Patient Safety incidents are triaged on an individual basis and will be shared with the relevant provider/lead for investigation where appropriate. Clinical quality incident trends, themes and lessons learned are reported to the CCG's Quality Committee 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 learnt for certain categories of incidents to other organisations. All serious incidents and DSP reportable 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. Implementation

All 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.

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.

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

7. Training Implications

The level of training required in incident reporting and management varies depending on the level and responsibility of the individual employee. Training requirements for staff groups are:

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

The CCG will ensure that the necessary training or education needs and methods required to implement the framework/procedure(s) 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.

8. Just Culture

The CCG supports a consistent, constructive and fair evaluation of the actions of staff involved incidents. The CCG considers a number of factors when investigating staff actions involved in an incident including but not exhaustive of:

- Deliberate harm
- Health (substance abuse, physical ill health, mental ill health
- Foresight (protocols, processes, procedures and the implementation)
- Substitution (experiences, qualification and training)
- Mitigating circumstances (any significant circumstances).

Just Culture 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

- 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' can be found at https://improvement.nhs.uk/resources/just-culture-guide/

8.1 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. All involved will be treated fairly.

During an incident investigation, appropriate support will be offered to staff and others 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 CSU Governance team.

9. Documentation

9.1 Other Related Documents

- Risk Management: Policy
- Anti-Fraud, Bribery and Corruption Policy
- Health & Safety policies and procedures
- Serious Incident Management policy
- Business Continuity Plan
- Standards of Business Conduct and Declarations of Interest policy
- Raising Concerns at Work policy
- Information Governance policies
- Complaints policy.

9.2 Legislation and Statutory requirements

- The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (HMSO) 1995
  Serious Incident Framework 2018 https://www.england.nhs.uk/patient-safety/serious-incident-framework
- Revised Never Events Policy and Framework 2018
  Revised Never Events policy and framework | NHS Improvement
- 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 Business Services Authority Whistleblowing Policy 2018
- Health and Social Care Act 2012.

9.3 References

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

10. Monitoring, Review and Archiving

10.1 Monitoring

The Governing Body will agree with the Executive Committee a method for the monitoring, dissemination and implementation of this framework.

10.2 Review

The Governing Body 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 Head of Corporate Services who 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.

10.3 Archiving

The CCG Governing Body 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.

11. 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: Julie Rutherford
Job Title: Senior Governance Officer
Organisation: NECS

Title of the service/project or policy: CO08 Incident Reporting and 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:
The policy provides information and guidance to staff working within the CCG to report and manage incidents and near misses.

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:

There are no potential negative impacts on protected groups as a result the development and implementation of this policy as it outlines the process for staff and service users to raise incidents and near misses and will therefore have a positive impact on promoting equal opportunities and eliminating discrimination.
As this is a staff policy, consideration in relation to accessibility will be given for CCG staff members who may have a disability, impairment or sensory loss and require information and correspondence in alternative formats they can easily access and understand, for example in audio, braille, easy read or large print.

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	☒	☐
If any of the above have not been implemented, please state the reason: Not applicable		

Governance, ownership and approval

Please state here who has approved the actions and outcomes of the screening		
Name	**Job title**	**Date**
Executive Committee	Approval Route	8th December 2020

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 Duties and Responsibilities

The Council of Members	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 documents.
Chief Finance Officer	The Chief Finance 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.
Accountable Officer	The Accountable Officer 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 learnt. •
Director of Nursing	The CCG Director of Nursing (or equivalent) has overall responsibility for ensuring the necessary management systems are in place for the effective implementation of patient safety clinical incidents and serious incident reporting for the CCG and delegates management of patient safety clinical incidents and SIs and reporting to the CSU Clinical Quality team.
CCG Corporate Investigating Manager	The CCG Corporate Investigating Manager has the responsibility to: • Support staff to maintain the incident policy and to manage individual incidents in accordance with policy; • Work closely with the accountable officer to ensure a transparent and consistent approach to incident management across the CCG in partnership with key stakeholders.
CSU Information Governance Lead / team / Data Protection Officer (DPO)	The CSU Information Governance Lead / team / DPO 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 • Work in collaboration with IT, develop, implement and monitor information security across the organisation • Support the CCG in evidence collation and upload for the DSP Toolkit.

All Staff	All staff, including temporary and agency staff, are responsible for: • Complying with relevant process documents. Failure 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 • Identifying 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 their line manager • Attending training/awareness sessions when provided.
Commissioning Support Unit	The CSU Governance team will: • Provide incident management support and advice • Produce CCG 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 / DSP incidents. The CSU Clinical Quality team 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 in relation to providers. The CQ team will manage these incidents according to the processes agreed with CCGs and Providers The 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.

Appendix 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 response and recovery arrangements to be undertaken to facilitate the resumption and restoration of activities.

Corporate Business Incidents
A corporate business incident is an event or circumstance that could have or did have a negative impact on the way the CCG conducts business with their stakeholders and/ or that could lead to financial loss.

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

Contractors
In relation to this policy, 'contractors' refers to agency staff, and employees of the CSU 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.

Corruption
Corruption can be broadly defined as the offering or acceptance of inducements, gifts, favours, payment or benefit-in-kind which may influence the action of any person. Corruption does not always result in a loss. The corrupt person may not benefit directly from their deeds; however, they may be unreasonably using their position to give some advantage to another.

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.

Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data

Personal data breaches include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data.

Fraud

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 for example such as invoices, to claim money they are not entitled to.

The Fraud Act 2006 created a criminal offence of fraud and defines three main ways of committing it:

- Fraud by false representation;
- Fraud by failing to disclose information; and,
- Fraud by abuse of position.

For fraud to occur the offenders conduct must be dishonest and their intention must be to make a gain, or cause a loss (or the risk of a loss) to another.

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,

Health and Safety, Fire, and Security Incidents

A health and safety, fire, or security incident is an event or circumstance that affects staff/visitors’ safety.

A reportable health and safety, fire & security incident will fall under one of the following categories:

- **Estates facilities** - could include a water leak, a lack of electricity occurring in buildings
- **Environmental** – impact on land, air or watercourses
- **Fire** - could include fire outbreak, false alarm
- **Security** - could involve damage, loss, theft
- **Staff accident** – e.g. slips, trips and falls, injuries to persons.

Information Governance (IG) / Data Security and Protection (DSP) Incidents

An information governance / data security and protection incident is an event or circumstance which adversely affects or could affect the security of the information maintained by the CCG.

IG incidents will fall in to one of the following cause groups:

- 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 / smartcard sharing.

Information Technology (IT) Incidents

An information technology (I.T.) incident is an event or circumstance that negatively affects or could negatively affect the way the CCG does business and is attributed to I.T. 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.

Near Miss

An incident could be a near miss which is an event or situation that has the potential to cause harm but did not occur. These events should also be reported as the organisation can learn lessons and can implement preventative action where required.

NHS Commissioning Board Special Health Authority

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

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.

The National Reporting and Learning System (NRLS)

The NRLS is a central database of patient safety incident reports. All information submitted is analysed to identify hazards, risks and opportunities to continuously improve the safety of patient care.

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 (SI) and Never Events
NHS England has produced an information resource to support the reporting and management of serious incidents

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:
    a. Suicide/self-inflicted death.
    b. Homicide by a person in receipt of mental health care within the recent past.

2. Unexpected or avoidable death of one or more 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 :
    a. The death of the service user
    b. Serious harm
    c. Actual or alleged abuse; sexual abuse, physical and 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

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/DSP related issues
    - Property damage
    - Security breach/concern, Article 4 (12) of the General Data Protection Regulations “Personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
    - Cyber incidents: The Security of Network and Information Systems Directive ("NIS Directive") requires reporting of relevant incidents to the Department of Health and Social Care (DHSC) as the competent authority from 10 May 2018
    - 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)
- Activation of Major Incident Plan (by provider, commissioner or relevant agency).

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

All incidents and Never Events should be reported on SIRMS in the first instance to be triaged for escalation via StEIS, DSP Toolkit, CareCERT etc.

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.

The CSU 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 learning from serious incidents in the near future.

Appendix 3

CCG Incident Assessment Matrix

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 risk matrix outlined below

1. Assessing the Incident

Step 1: Determine the consequence score of Incidents

From the submitted incident make a note of the cause group and use the corresponding tables (Tables 1-5) below to assess the consequence rating, the number is given at the top of the column.

The consequence score 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

NOTE	Any incident with a consequence score of 4 (major) or 5 (catastrophic) needs to be referred immediately to the responsible Chief Officer and the CCG Corporate Investigating Manager. An immediate management response is required. The incident needs to be recorded on SIRMS. Once recorded on SIRMS the above contacts will be notified automatically.

Consequence and Likelihood Scoring Matrix

Operational, Reputational and Financial Scoring Matrix

	Impact score (consequence/severity levels) and examples of descriptors				
	1	**2**	**3**	**4**	**5**
Descriptor	**Negligible (very low)**	**Minor (low)**	**Moderate (low)**	**Moderate (high)**	**High**
Operational	Minor reduction in quality of treatment or service. No or minimal effect for patients / customers	Single failure to meet national standards of quality of treatment or service. Low effect for small numbers of patients / customers	Repeated failure to meet national standards of quality of treatment or service. Moderate effect for multiple patients / customers if unresolved.	Ongoing non-compliance with national standards of quality of treatment or service. Significant effect for numerous patients / customers if unresolved.	Gross failure to meet national standards with totally unacceptable levels of quality of treatment or service. Very significant effect for a large number of patients if unresolved.
Reputational	Not relevant to mandate priorities. No adverse media coverage. Recognition from the public.	Minor impact on achieving mandate priorities. Low level of adverse media coverage. Small amount of negative public interest.	Moderate impact on achieving mandate priorities. Moderate amount of adverse media coverage. Moderate amount of negative public interest.	High impact on achieving mandate priorities. High level of adverse media coverage. Negative impact on public confidence.	Mandate priorities will not be achieved. National adverse media coverage. Total loss of patient / customer confidence.
Financial	Small loss where risk of claim is remote	Loss of 0.1% - 0.25% of budget where claims are less than £10,000	Loss of 0.25% - 0.5% of budget where claims are between £10,000 - £100,000	Uncertain delivery of key objective / loss of 0.5% - 1.0% of budget. Claim(s) between £100,000 and £1 million. Purchasers failing to pay on time.	Non-delivery of key objective. Loss of more 1% of budget. Failure to meet specification / slippage. Loss of contract / payment by results. Claim(s) of more than £1 million.

Step 2 - Timeline for Managing Incidents

1	**Negligible/no harm** Incident to be noted and closed off within 5 days by the CCG Appointed Incident Investigating Officer.
2	**Low risk** CCG Appointed Incident Investigating Officer to manage and close off the incident within 5 days.
3	**Medium risk** - The CCG Appointed Incident Investigating Officer will manage and close off the incident within 5 days.
4	**High risk** Once recorded these incident must be referred immediately to the Chief Officer, CCG Corporate Investigating Manager and a CSU Specialist Officer. A management response is required as soon as possible within a 24 hour period. The Chief Officer to close off the incident within 1 month. If the close off target is not met an interim report of progress needs to be submitted to the CCG Corporate Investigating Manager.
5	**Catastrophic** Once recorded these incident must be referred immediately to the Chief Officer, CCG Corporate Investigating Manager and a CSU Specialist Officer. A management response is required as soon as possible within a 24 hour period. The Chief Officer to close off the incident within 1 month. (If the close off target is not met an interim report of progress needs to be submitted to the CCG Corporate Investigating Manager.
6	Near Miss – This incident need to be referred to the reporter's manager to decide the seriousness of the incident should the near has miss occurred. If the reporter's manager thinks the incident would have been significantly serious and could happen again, a RCA will be required to reduce the likelihood of the incident re-occurring. If the incident needs an RCA the incident should be closed within 1 month of the near miss occurring. If the near miss is not serious manage the incident as routine and close the incident within 5 days on SIRMS
7	Soft Intelligence – This incident is recorded for information and should be reported and closed with 5 days.