NHS
North East and North Cumbria

Corporate	ICBP020 Incident Reporting and Management Policy

Version Number	Date Issued	Review Date
1	July 2022	January 2023

Prepared By:	Senior Governance Officer, North of England Commissioning Support
Consultation Process:	Integrated Governance Workstream
Formally Approved:	July 2022
Approved By:	Executive Committee

EQUALITY IMPACT ASSESSMENT

Date	Issues
June 2022	None

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.

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 NECSU.comms@nhs.net

Version Control

Version	Release Date	Author	Update comments
1	July 2022	Senior Governance Officer	First Issue

Approval

Role	Name	Date
Approver	Executive Committee	July 2022

Contents

1. Introduction

The Integrated Care Board (ICB), Incident Reporting and Management Policy sets out its approach to the management of incidents in fulfilment of its strategic objectives and statutory obligations.

The ICB 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. To provide clear and consistent guidance, the ICB will develop documents to fulfil all statutory, organisational, and best practice requirements.

The ICB is responsible for ensuring incidents are robustly managed to improve the quality of services it provides and partnerships its established, so that they are well governed, safe and of a high standard. The ICB is responsible for ensuring their employees (permanent, fixed term), partners and contractors have effective systems in place to identify and manage incidents and risks to support their development where necessary.

The ICB act as a conduit for information, around incidents and risks to ensure learning (and the opportunities for risk reduction) is not lost within the ICB or the wider NHS.

This policy sets out the approach taken by the ICB in the management of incidents in fulfilment of its strategic objectives and statutory obligations. The reporting of incidents will help the ICB to identify potential breaches and weakness in controls in its core business including breaches in:

- Contractual obligations
- Internal processes
- Statutory duties
- Partnership Governance (where the ICB is the accountable body)

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

The ICB aims to develop an open learning culture of incident reporting, based on the principles of fair blame. Staff should not be afraid of raising concerns and will not experience any blame recrimination as result of making any reasonably held suspicion known.

This policy covers the reporting and management of the following types of incidents:

- Corporate business incidents
- Health and safety / fire / security or environmental incidents
- Information Governance incidents
- IT (Information Technology)/Cyber Security incidents
- Incidents that impact patient safety

The policy interlinks with ICB Serious Incidents (SIs) Management Policy for the reporting and management of serious incidents and the ICB Business Continuity Plan.

An effective integrated incident management framework will ensure that the reputation of the ICB is maintained, enhanced, and its resources used effectively to ensure business success, financial strength, and continuous quality improvement.

2. Purpose and Scope

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

- Providing guidance on the process for reporting and managing incidents for employees and contractors (supported by the Incident Reporting and Management SOP)
- Setting out the roles and responsibilities of ICB employees, contractors committees and the organisation 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 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 Learning from Patient Safety Events (LFPSE) Integrating where relevant existing ICB policies including the Serious Incidents Management Policy the Business Continuity Plan and the Counter Fraud Bribery and Corruption Policy.

3. 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 ICB incident could involve:

- The environment (workplace)
- Organisational reputation.
- Property
- Service delivery
- Staff
- Stakeholders.

The incident might impact different aspects of ICB operations for example its:

- Reputation
- Resources
- Staff and Contractors
- The quality of services the ICB provides and commissions

4. Reporting an Incident

All ICB employees (permanent, fixed term etc.) have a duty to report all clinical and non-clinical incidents they are involved in, witness or have an awareness of. All ICB employees should report incidents using the electronic on-line reporting system – The Safeguard Incident and Risk Management System, (SIRMS).

For most staff, SIRMS can be accessed at this web-address:
https://sirms.necsu.nhs.uk

Full guidance on how to report and manage an incident via the web-form can be found in the ICB incident management SOP

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

5. Management of 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 ICB, however the ICB might ask CSU colleagues to undertake this on its behalf. Specific duties are outlined in the duties and responsibilities section of this policy.

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

It is the responsibility of the ICB nominated Corporate Investigating Manager to identify who is the most appropriate person to action the incident and complete the management form. The management of the incident will also include, setting and implementing actions to mitigate further risk of the incident happening again.

Management of incidents and risks through SIRMS is interdependent, however risks can be identified through the monitoring of incident themes and trends. If a particular type of incident continues to occur, this may indicate that a risk around the root cause of the incident, would need to be reported on the relevant ICB risk register.

Both clinical and non-clinical incident reports are reviewed, as agreed, at the ICB's (committee to be inserted).

6. Investigation of Significant Incidents & Serious Incidents (SIs)

An incident with an impact score on SIRMS of 5 (catastrophic) or 4 (major) indicates the reported incident is significant and should be reported immediately to the Chief Executive and the ICB Head of Corporate Services, who will appoint the Investigating Officer, to carry out a formal investigation to establish the root cause of the incident is required.

The ICB's standard approach for investigating a significant incident is to carry out a Root Cause Analysis (RCA) to establish the root cause of the incident and to prevent the incident from re-occurring in the future. The SIRMS ICB Incident Reporting and Management SOP provides further information and guidance in relation to RCA principles including the RCA investigation template.

7. StEIS Reportable Incidents

To ensure all ICB significant incidents are given due attention all reported ICB significant incidents (with an incident impact score or 4 or 5), will be forwarded by the CSU Governance team to the CSU Clinical Quality Team to consider if the incident requires to be reported onto the Strategic Executive Information System (StEIS) as a Serious Incident (SI). StEIS is the national reporting system for

incidents that fall into the category of a SI according to the definitions set out in the NHSE Serious Incident Framework 2015.

Examples of a StEIS reportable SI includes patient safety issues where there has been serious harm but can also include incidents such as IT/Cyber Security incidents, Health and Safety Incidents, Patient Identifiable Data breaches and incidents that result in a major loss of confidence in the organisation, including prolonged adverse media coverage or public concern about the quality of healthcare or of an organisation.

If the incident is found to be StEIS reportable, it will be reported on StEIS by the CSU Clinical Quality Team according to the processes set out in the ICB Serious Incident Management Policy, where information on the definition and management of SIs can also be obtained.

8. Incidents related to Personal Confidential Data

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.

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

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

If a data processor suffers a breach, then under Article 33(2) it must inform the controller without undue delay as soon as it becomes aware. This allows the controller to take steps to address the breach and meet breach-reporting obligations under the GDPR. The requirements on breach reporting should be detailed in the contract between the controller and the 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 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, 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 IG team will support the ICB in evidencing, collating, and uploading a DSP reportable incident on the DSP Toolkit.

As a guide DSP Reportable high-risk incident could be any incident which involves actual or potential failure to meet the requirements of the Data Protection Act 2018 or UK General Data Protection Regulation) and/or Common Law Duty of Confidentiality. Incidents could include:

- The unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people's privacy
- Personal data breaches which could lead to identity fraud or have other significant impact on individuals; and
- Applies irrespective of the media involved and includes both electronic media and paper records.

The CSU IG Team reviews DSP incidents reported by the ICB 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 ICB Incident Manager manages updates and closes DSP reportable incidents on the Incident Reporting and Management Module of SIRMS, rather than the CSU IG team.

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 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.
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:

- 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 was 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.

9. IT /Cyber Incidents

The ICB works with its staff, the CSU, to ensure Cyber Security measures are actively in place to protect services, services users, and partners, should a critical cyber incident occur. The incident procedures the ICB have in place facilitates the organisation learning lessons from cyber/IT related incidents, and ensures actions are in place to mitigate the risk of critical cyber incident happening again.

The ICB and CSU incident procedures provide assurance to the organisation, that critical cyber security incidents are managed as a Board level risk.
The ICB and the CSU work with colleagues in NHS Digital to confirm the organisation is aware of their accountabilities and responsibilities should cyber security incidents, occur. This approach provides assurance on the readiness of the ICB and the CSU.

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 CSU IT service desk and the ICB’s IT lead should be informed. The CSU Business Information Services will assess these incidents to determine whether they need to be reported in line with Network and Information Systems Regulations (NIS).

10. RIDDOR

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 into this category staff should email the CSU Health and Safety Specialist at: necsu.healthandsafety@nhs.net who can then advise accordingly.

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

11. Clinical Quality Incidents

Clinical quality incidents occur when:

- An issue is identified in which patients or service users experience actual or potential harm as a result of clinical services provided by ICB employees, and;
- An issue is identified in which an organisation commissioned by the ICB to provide clinical services causes, or has the potential to cause, harm to patients or service users.

It is expected that as the number of clinical services delivered by the ICB will be limited, there will be very few of the former type. ICB staff should, however, use SIRMS to report clinical quality incidents that they become aware of involving provider organisations such as NHS Trusts, GP Practices, Pharmacies and Care Homes etc. Incidents of the latter type will be included in the larger clinical quality commissioning intelligence data that is reported by GP Practices and Trusts across the North East and North Cumbria in order to identify quality concerns and promote improvements across the system.

Staff have a duty to report any clinical quality incidents that they witness or are involved in. To report these, staff are instructed to use the ICB/Provider incident reporting page of SIRMS - https://sirms.necsu.nhs.uk/

The CSU Clinical Quality Central Incident Team (CIT) leads the management of clinical quality incidents reported by both the ICB and providers including GP Practices, GP Federations, Trusts, Hospices and Primary Care Networks. The CSU CIT manages all clinical quality incidents reported on SIRMS on a daily basis and clinical quality incidents reported about other providers will generally fall into one of the following pathways:

- Thematic Incidents – low risk and high volume trends or themes across similar incident types, identifying systematic or process issues in an organisation, and;
- Incidents Requiring an Individual Response – high risk and low volume and typically involving a single patient and requiring a response from the organisation in which the incident occurred.

The CSU Clinical Quality Team is responsible for updating the SIRMS record with the action taken to manage the incident following triage into the appropriate pathway (for example if the incident was referred to a provider for further investigation).

Further progress updates on SIRMS will depend on where the incident has been referred and whether the organisation investigating and resolving the incident can access SIRMS. The CSU Clinical Quality Team follow-up incidents reported to external providers to ensure the incident is being satisfactorily managed and to ensure that where required a response is obtained for the reporter.

The CSU Clinical Quality team will consider in conjunction with the relevant senior managers in the ICB if an ICB significant incident falls into the category of a StEIS reportable Serious Incident. Advice on whether an incident meets the StEIS reportable criteria can be sought from NECS Clinical Quality Team for clinical quality issues or the NECS IG Team for patient data protection issues. The CSU Clinical Quality team is responsible for identifying and recording serious incidents on STEIS on behalf of the ICB, GP Practices and any independent providers without direct access to the national reporting system.

12. Corporate Incidents

The ICB, as commissioners, seek to assure that all services they commission or directly provide meet national identified standards, and ensure that this is managed through their contracting process. The impact of a corporate incident could lead to a financial loss or a negative impact on the reputation of the organisation.

Corporate business incidents that are reportable would likely include one or more of the following concerns:

- A lack of staff to meeting commissioning responsibilities
- A business quality concern
- A communications breakdown
- A significant lapse in KPIs or agreed standards
- A failure to meet a statutory requirement
- An incident related to the CCG transition to ICB
- An incident associated with a partnership or service level agreement.

Corporate business incident trends, themes and lessons learned will be reported to the ICB's Committee:

- Audit Committee
- Governing Board

12 Fraud and Corruption

Under no circumstances should suspicions of fraud, bribery or corruption be recorded as an incident in SIRMS. For details how to report these refer to the ICB's Counter-Fraud, Bribery and Corruption Policy.

13. Freedom to Speak Up

To support employees in reporting suspicions the ICB has a Raising Concerns at Work (Whistleblowing) Policy, which is available to all staff.

14. Level of Investigation

It is the responsibility of the ICB 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. Information around external incidents is useful for the ICB, as a commissioner, as it can be used as commissioning intelligence to support service delivery discussions.

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. All incidents with an initial impact assessment of 4 or 5 require an RCA investigation and are classified as serious or significant.

15. Onward reporting

Occasionally, the ICB will be required to onward report trends and lessons learnt for certain categories of incidents to other organisations. All serious/significant, 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:

LFPSE	Learning From Patient Safety Events) 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
Cyber Security	Reported in line with Network and Information Systems Regulations (NIS).

16 Just Culture

The ICB supports a consistent, constructive, and fair evaluation of the actions of staff involved incidents. The ICB considers several 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 do 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/

17. Implementation

All managers are responsible for ensuring that relevant staff within the ICB 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 ICB Board 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.

18. 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	Managers.

The ICB 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.

19. 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.

20. Related Documentation

- Risk Management: Policy
- Counter-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.

21. 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.

22. Monitoring, Review and Archiving

Monitoring

The ICB Board will agree with the Executive Committee a method for the monitoring, dissemination and implementation of this Policy framework.

Review

The ICB Board or a nominated Committee 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 Sponsoring Director 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.

Archiving

The ICB Board 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.

Schedule of Duties and Responsibilities

Through day-to-day work, employees are in the best position to recognise any specific fraud risks within their own areas of responsibility. They also have a duty to ensure that those risks, however large or small, are identified and eliminated. Where it is believed fraud, bribery or corruption could occur, or has occurred, this should be reported to the CFS or the chief finance officer immediately.

ICB Board	The ICB Board has responsibility 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.
Accountable Officer/Chief Executive	The Chief Executive has overall responsibility for the strategic direction and operational management, including ensuring that ICB process documents comply with all legal, statutory, and good practice guidance requirements.
The Senior Governance Officer, NECS	The Senior Governance Officer, NECS will ensure that the policy is updated according to the agreed timetable for review, or whenever significant changes occur in the statutory frameworks.
[Titles of relevant officers]	The titles of any officers who have specific responsibility for implementation of any part of the process, clearly stating what that person's responsibility is, including who is responsible for drafting and updating any part of the document.
Commissioning Support Staff.	Whilst working on behalf of the ICB CSU staff will be expected to comply with all policies, procedures and expected standards of behaviour within the ICB, however they will continue to be governed by all policies and procedures of their employing organisation.
All Staff	All staff, including temporary and agency staff, are responsible for: • Compliance with relevant process documents. Failure to comply may result in disciplinary action being taken. • Co-operating with the development and implementation of policies and procedures and as part of their normal duties and responsibilities. • Identifying the need for a change in policy or procedure because of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising their line manager accordingly. • Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager. • Attending training / awareness sessions when provided.

Appendix A – Equality Impact Assessment

Equality Impact Assessment
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: Click here to enter text.

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

What are the aim(s) and objectives of the service, project or policy:
This policy aims to ensure that the ICB as Commissioners comply with current legislation as well as current national guidance, NHS England guidance and requirements with regard to accident/incident reporting and managing generally, this includes reporting, notifying, managing, and investigating Serious Incidents

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

- **Staff** ☒
- **Service User / Patients** ☐
- **Other Public Sector Organisations**☐
- **Voluntary / Community groups / Trade Unions** ☐
- **Others, please specify** Click here to enter text.

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

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

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 NECS 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	☒	☐
Please provide the following caveat at the start of any written documentation: **"If you require this document in an alternative format such as easy read, large text, braille or an alternative language please contact (ENTER CONTACT DETAILS HERE)"**		
If any of the above have not been implemented, please state the reason: NA		

Governance, ownership and approval

Please state here who has approved the actions and outcomes of the screening		
Name	**Job title**	**Date**
Julie Rutherford	Senior Governance Officer	June 2022

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.

If you are not completing 'STEP 2 - Equality Impact Assessment' this screening document will need to be approved and published alongside your documentation.

Please send a copy of this screening documentation to:
NECSU.Equality@nhs.net for audit purposes.