Nottingham and Nottinghamshire Integrated Care Board

Incident Reporting and Management Policy[1]

May 2024 – May 2027

[1] This Policy should be followed for all ICB corporate incidents, which include Health and Safety, Security and Information Governance incidents.

CONTROL RECORD	
Title	Incident Reporting and Management Policy
Reference Number	H&S-004
Version	2.0
Status	Final
Author	Head of Corporate Assurance; Head of Information Governance
Sponsor	Director of Corporate Affairs
Team	Corporate Assurance; Information Governance
Amendments	To include Caldicott Guardian and Information Asset Owners at Section 5. To include Serious Incidents at Section 16.
Purpose	To ensure that a robust reporting and management system is in place for incidents, accidents and near misses occurring within NHS Nottingham and Nottinghamshire Integrated Care Board. This policy also references the requirement to report to external organisations, where necessary (e.g. the Information Commissioner's Office or the Health and Safety Executive).
Superseded Documents	Incident Reporting and Management Policy v1.3
Audience	All employees and appointees of the ICB and individuals working within the organisation in a permanent or temporary capacity.
Consulted with	Health, Safety and Security Steering Group; Information Governance Steering Group.
Equality Impact Assessment	Completed
Approving Body	Audit and Risk Committee
Date approved	16 May 2024
Date of Issue	May 2024
Review Date	May 2027
This is a controlled document and whilst this policy may be printed, the electronic version available on the ICB's document management system is the only true copy. As a controlled document, this document should not be saved onto local or network drives.	

NHS Nottingham and Nottinghamshire Integrated Care Board (ICB)'s policies can be made available on request in a range of languages, large print, Braille, audio, electronic and other accessible formats from the Engagement and Communications Team at nnicb-nn.comms@nhs.net.

Contents

Appendices:

1. Introduction

1.1. This policy applies to NHS Nottingham and Nottinghamshire Integrated Care Board hereafter referred to as 'the ICB'.

1.2. This document sets out the approach to the reporting, management and investigation of all corporate incidents (including accidents and near misses) that occur within the organisation. Corporate incidents, internal to the ICB, may relate to Health and Safety, security or Information Governance (such as personal data breaches). **Separate guidance is in place within the ICB's Nursing Directorate on how to manage incidents which occur within the services we commission from our providers.**

1.3. Incident management is a cyclical process that requires the identification and reporting of incidents; followed by investigation (if necessary), remedial action and learning to mitigate the risk of recurrence. The reporting of all incidents (or the potential for incidents) no matter how trivial they may appear will enable the ICB to build a profile of risks to staff, the public and to the business of the organisation.

1.4. This policy also describes where incidents may require reporting to external bodies (e.g. the Information Commissioner's Office, NHS Digital, the Health and Safety Executive etc) and the individual responsibilities in relation to this. The organisation will always adhere to the national requirements if such an incident should occur.

2. Purpose

2.1. The purpose of this policy is to:

- Ensure that robust incident reporting mechanisms are in place so that all corporate incidents are captured and managed in a systematic way.
- Ensure that any regulatory requirements in relation to incident reporting are fulfilled.
- Ensure that all staff have a clear understanding of their responsibilities.
- Enable the ICB to learn lessons from incidents through the implementation of actions to prevent incidents from reoccurring.
- Encourage a reporting and questioning environment within the organisation that gives staff the confidence to report incidents and openly discuss working practices.

3. Scope

3.1. This policy relates to all employees and appointees of the ICB and others working within the organisation in a temporary capacity. It also applies to ICB employed staff who carry out work within another organisation's premises. These are collectively referred to as 'individuals' hereafter.

4. Definitions

4.1. For the purposes of this policy, all of the following will hereby be referred to as 'incidents' unless the process for the management of serious incidents differs significantly.

Term	Definition
Incident	An incident can be described as an event that has, or may have, an adverse outcome for an individual or the organisation. Examples of incidents that may occur within a commissioning organisation may relate to (but are not limited to) the following areas: • Information governance (e.g., the unauthorised or inappropriate disclosure of person identifiable data or the loss of unencrypted IT equipment that contains personal or sensitive data). • Health and safety (e.g., an accident that occurred during working activities or unsafe working practices). • Security (e.g., theft or unauthorised access to premises). • Aggression (e.g., verbal abuse). The incident may impact different aspects of the ICB operations, for example, its reputation, resources, staff and contractors.
Accident	An accident is an unplanned or unexpected event that resulted in, or could have resulted in, injury or harm to staff or visitor.
Near miss	A near miss can be described as an event where one of the above almost occurred or had the potential to occur.

5. Roles and Responsibilities

Role	Responsibilities
Integrated Care Board	Has ultimate responsibility for the ICB risk management arrangements. Incident management is integral to the management of risk and, therefore, the ICB needs to be satisfied that appropriate policies and procedures in relation to this are in place. The ICB also has a duty to promote a culture of transparency and openness, where it is acceptable and safe for staff to report all incidents.
Audit and Risk Committee	Has delegated responsibility for overseeing the ICB risk management arrangements and as such; will maintain a strategic overview of all reported incidents and ensure that appropriate management actions have been taken in response.

Role	Responsibilities
Health, Safety and Security Steering Group	Has responsibility for ensuring that arrangements for managing and appropriately responding to corporate incidents and/or near misses are in place; and that staff are appropriately trained and aware of their responsibilities.
Information Governance Steering Group	Has responsibility for ensuring arrangements for proactively preventing data security breaches and responding to, and ensuring learning from, incidents and near misses.
Chief Executive	Has overall responsibility for the management of serious incidents, including responsibility for the appropriate closure of serious incident files.
Senior Information Risk Owner (SIRO)	Has responsibility for owning the ICB information governance management framework, ensuring that the ICB approach to information risk management is effective in terms of clear lines of responsibility and accountability, resources, commitment and execution and that this approach is communicated to all staff.
Caldicott Guardian	Has responsibilities to make sure that the personal information is used legally, ethically and appropriately, and that confidentiality is maintained.
Information Asset Owners	Are responsible for ensuring that specific information assets are accessed, handled and managed appropriately.
Head of Information Governance	Supported by the SIRO, will also ensure that effective mechanisms are established and publicised for responding to and reporting Information Governance Serious Incidents and Cyber Serious Incidents requiring investigation.
Head of Corporate Assurance	Has a responsibility to ensure that**:** • Systems and processes are in place for the reporting and management of all corporate incidents and that these arrangements are effective and fit for purpose. • The incident risk rating is an accurate reflection of any residual risk. • The appropriate level of investigation and onward reporting has been carried out for all reported incidents. • The incident database is maintained and reports are available to inform the work of committees. • Staff are advised and supported accordingly during

Role	Responsibilities
	the reporting and any ensuing investigation of incidents. • Ensuring that learning from all incidents is fed back to staff via the ICB's staff communication processes.
Data Protection Officer (DPO)	Has responsibility for monitoring internal compliance with Data Protection obligations and to act as a point of contact for data subjects and the supervisory authority.
All Staff	Have a responsibility for: • Reporting incidents in accordance with this policy. • Co-operating and participating fully in any incident investigations that take place.

6. Fair Blame

6.1. The ICB is committed to learning from all incidents and in ensuring a safe and effective organisation for its staff, visitors and anyone else who may be affected by the ICB's activities. This policy is in place to support staff in the reporting of incidents without any fear of recrimination.

6.2. The ICB accepts that incidents can sometimes occur due to human error and under this policy; blame will not be apportioned to any individual where this may be the case. However, this does not extend to incidents that have occurred as a consequence of misconduct, gross negligence or an act of deliberate harm. Incidents resulting from these circumstances will be dealt with in accordance with the organisation's disciplinary policies and procedures.

7. Reporting Corporate Incidents (non-IG incidents)

7.1 The reporting of incidents is an important means of providing information that allows the organisation to investigate such occurrences quickly. It helps with the process of identifying the causes of such incidents from which lessons can be learned and control measures put in place to reduce the risk of recurrence. Guidance on the actions to be taken immediately after a non-information governance incident can be found on the flowchart provided at **Appendix A**.

7.2 All incidents should be reported to the line manager as soon as possible after the event. If the line manager is not available, report the event to the most senior member of staff available.

7.3 The Head of Corporate Assurance and/or Head of Information Governance will ensure that any necessary reports to regulatory and professional bodies have been made.

7.4 Specific reporting requirements in relation to an information governance, or personal data breach, are provided at **Appendix B** of this policy.

7.5 The person involved in the incident or who has identified the incident should complete the Incident Report Form**.** In instances where a member of staff is unable to complete the form due to illness or injury, the senior person on duty should complete the incident report form.

7.6 All incidents should be recorded and forwarded to the Head of Corporate Assurance within an appropriate timescale following the incident occurring or being identified (via email at nnicb-nn.corporateassurance2@nhs.net.

7.7 Some work-related accidents and diagnosis of certain occupational diseases may require reporting to the Health and Safety Executive under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR).

7.8 Where the Health and Safety Executive or other external bodies (e.g. the Police) may need to be informed, a member of the Executive Management Team will determine who should contact the relevant organisation.

7.9 The Head of Corporate Assurance will be responsible for following up the incident within an appropriate timescale. This will ensure that any subsequent actions have been completed and that the incident is recorded and reported within the ICB accordingly

8. Initial Management of the Incident

8.1 Depending on the type of incident, the following actions should be taken where appropriate:

- Attend to the immediate health needs of the individual(s) without endangering yourself. Arrange any first aid or medical care as needed.
- Make the situation safe - take out of use and retain any equipment deemed faulty.
- Make contact with emergency services where required.
- Inform the Police if there has been a violent or criminal act.
- Inform the line manager or an appropriate senior member of staff.

9. Information Governance Incidents: Personal Data Breaches

9.1. Under the Data Protection Act 2018 (DPA) and the General Data Protection Regulation 2016 (GDPR) the ICB must report any data breach which is likely to result in a high risk to data subjects' rights and freedoms, within 72 hours to the Information Commissioner's Office (ICO).

9.2. A personal data breach is defined as ‘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’.

9.3. Personal data breaches may also relate to incidents involving security of the network or information systems and includes cyber incidents.

9.4. The Security of Network and Information Systems Regulations 2018 (NIS Regulations) seek to ensure that essential services, including healthcare, have adequate data and cyber security measures in place to deal with the increasing volume of cyber threats.

9.5. The NCSC (National Cyber Security Centre) defines a cyber-incident as a breach of a system's security policy in order to affect its integrity or availability and/or the unauthorised access or attempted access to a system or systems; in line with the Computer Misuse Act (1990).

9.6. The ICB is also required to report data breaches or incidents under the NIS Regulations to the Department of Health and Social Care through the NHS Digital Data Security and Protection Toolkit (DSPT) and comply with the NHS Digital Guide to the Notification of Data Security and Protection Incidents.

9.7. It is a legal requirement to do this reporting and a failure to report promptly could result in substantial fines under data protection legislation or NIS Regulations.

9.8. It is essential that staff identifying an actual or potential data breach inform their manager without delay and complete the Information Governance Incident Report Form at Appendix E. The reporting and subsequent investigation of an Information Governance (IG) breach is separated into three parts.

- **IG Report Form (Part 1)** to be completed as soon as possible for all Information Governance (IG) Information Security, Cyber Security Incidents or Near Misses as set out in Section 9. The form should record the factual details of the incident and details of any immediate actions
- **IG Incident Investigation Form (Part 2)** to be completed by manager following Individuals completing this form. Please contact the IG Team for guidance **nnicb-nn.igteam@nhs.net**.
- **IG Team Risk Assessment and Reporting Form (Part 3)** to be completed by the IG Team.

9.9. The ICB’s Information Governance Team must also be informed as soon as possible at nnicb-nn.igteam@nhs.net to ensure they can assess the situation and ensure prompt action to limit or prevent any potential harm or damage and determine if the data breach meets the criteria for external reporting.

9.10. Upon receipt of the incident report, the Head of Information Governance will notify the ICB’s SIRO, Caldicott Guardian and Information Asset Owner (IAO) as relevant.

9.11. The Head of Information Governance will be responsible for following up the incident within an appropriate timescale. This will ensure that any subsequent actions have been completed and that the incident is recorded and reported

within the ICB accordingly.

10. External Stakeholder Notification

10.1 Certain types of incidents, in addition to being reported within the organisation, are also reportable under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR).

10.2 Cases of work-related incidents which result in an absence from work for more than seven consecutive days must be reported under RIDDOR within fifteen days of the incident occurring.

10.3 The Chief Executive, supported by the Head of Corporate Assurance, will be responsible for the reporting of RIDDOR incidents.

10.4 The Head of Information Governance in conjunction with the Director of Corporate Affairs, SIRO and Caldicott Guardian, as appropriate, will determine whether any internal information governance or cyber security incidents meet the criteria for external reporting via the Data Security and Protection Toolkit (DSPT). Reporting via the DSPT will automatically inform external stakeholders (e.g. the Information Commissioner's Office, NHS Digital).

10.5 Examples of other external agencies that may require notification of an incident (dependant on the nature of the incident) are shown below:

- Police;
- Local Authority;
- Professional Regulatory Bodies;
- NHS Property Services;
- NHS Resolution;
- Counter Fraud and Security Management Services.
- Information Commissioner's Office
- NHS Digital

11. Incident Grading

11.1 All incidents, with the exception of those relating to Information Governance, must be graded using the risk assessment matrix **(Appendix C)** to reflect the potential impact of the incident in respect of loss/damage/injury (actual or potential) and the likelihood of a recurrence. The grading should be undertaken on the basis of the facts known at that point in time and following reasonable enquiry. For incidents that have been graded as serious, see section 15 for additional information.

11.2 Information Governance incidents are required to be graded using the matrix in NHS Digital Guide to the Notification of Data Security and Protection Incidents (SIRI Guide 2018) (**Appendix D**). The guidance sets out the actions required when a

personal data breach or Cyber Security SIRI occurs and stipulates a requirement to report externally to the Information Commissioner's Office and Department of Health and Social Care once a specific threshold has been met, based on the scoring outcome of the impact vs. likelihood.

12. Incident Investigation

12.1 It is essential that all incidents are reviewed. Whether the incident requires further investigation, and the level of this, is dependent on the nature of the incident and the potential for recurrence.

12.2 **Appendix C** provides guidance on the level of investigation required dependent on the risk score.

13. Learning from Incidents

13.1 Subsequent actions and learning from experience are key outputs from any incident investigation. In order to ensure a safe and effective organisation, it is important that any lessons learnt and changes to policies and procedures are communicated across the organisation. This will be performed through the relevant forum, i.e. team meetings, newsletters and email.

13.2 An inability to demonstrate learning from previous incidents will be taken seriously by regulatory authorities if previous warnings have been ignored.

14. Media Involvement

14.1 Where potential media interest exists, this will be dealt with by the Head of Communication, in conjunction with the Chief Executive or a delegated member of the Executive Management Team. Other members of staff will be consulted as appropriate.

15. Serious Incidents (non-IG incidents)

15.1 A Serious Incident Investigation Team (SIT) will be convened comprising of:

- A member of the ICB Senior Management Team
- Head of Corporate Assurance
- Lead Manager (of affected area/department)
- Specialists from other departments as required (such as Communications, Information Governance, Counter Fraud etc.)
- A member of the ICB Nursing Team to provide expertise regarding root cause analysis review and clinical quality/patient safety if required.

15.2 The membership of the Team will be increased to include representation from the areas affected, according to the nature of the incident.

15.3 The principle functions of the SIT are:

- Investigation of the serious incident (SI) to identify, as rapidly as possible, the facts and consequences, using RCA methodology. A timeline will be produced based on the SI and if necessary written statements gained.
- Co-ordinate information, communication and press coverage as well as establishing efficient means of dealing with enquiries from press, media, relatives and members of the public.
- Organise appropriate counselling and support for employees affected by the SI.
- Production of an action plan designed to correct or limit the consequences, minimise the chance of recurrence in the future and allow lessons to be learned.
- Production of a preliminary and final written report in a timely fashion under the guidelines set out in the national framework.

15.4 An investigating officer (Lead Investigator) must be appointed to manage the investigation, gather the facts of the SI, co-ordinate all statements and documentation, keep contemporaneous notes of the investigation meetings and ensure that the timescales set out in this policy are adhered to.

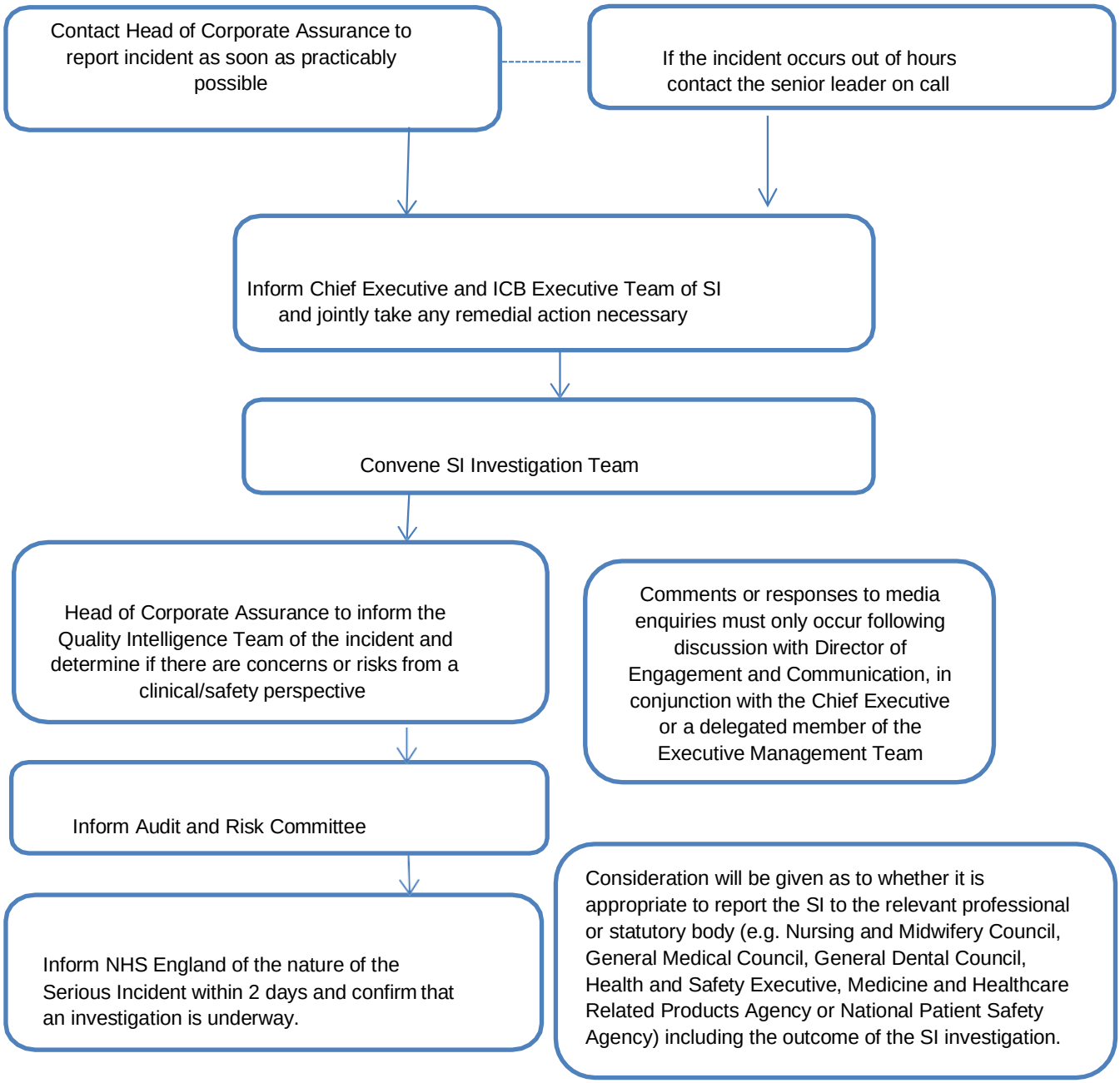
15.5 All serious incident reports will be sent to the ICB or delegated Committee for review, comment and action. They will be sent again once the action plan is complete so the committee can seek assurance.

15.6 The following flowchart (at Table 1) outlines the process to follow when reporting a serious incident.

15.7 Whilst the ICB fosters an open and supportive culture, it is acknowledged that in some instances an individual may have concerns regarding an incident or potential incident which he or she does not feel comfortable about reporting formally.

15.8 The ICB recognises that staff may want to raise a concern in confidence and issues raised in this manner will be addressed in accordance with the organisation's Standards of Business Conduct Policy.

Table 1


Contact Head of Corporate Assurance to report incident as soon as practicably possible
If the incident occurs out of hours contact the senior leader on call
Inform Chief Executive and ICB Executive Team of SI and jointly take any remedial action necessary
Convene SI Investigation Team
Head of Corporate Assurance to inform the Quality Intelligence Team of the incident and determine if there are concerns or risks from a clinical/safety perspective
Comments or responses to media enquiries must only occur following discussion with Director of Engagement and Communication, in conjunction with the Chief Executive or a delegated member of the Executive Management Team
Inform Audit and Risk Committee
Inform NHS England of the nature of the Serious Incident within 2 days and confirm that an investigation is underway.
Consideration will be given as to whether it is appropriate to report the SI to the relevant professional or statutory body (e.g. Nursing and Midwifery Council, General Medical Council, General Dental Council, Health and Safety Executive, Medicine and Healthcare Related Products Agency or National Patient Safety Agency) including the outcome of the SI investigation.

16. Serious Incidents (Information Governance)

16.1 Serious information governance incidents are determined in line with the NHS Digital “Guide to the Notification of Data Security and Protection Incidents”, 2018.https://www.dsptoolkit.nhs.uk/Help/Attachment/148

16.2 The guide is compliant with legal requirements which stipulate where serious information incidents have occurred, they must be reported to the Supervisory Authority within 72 hours of identification. Where the organisation notifies the ICO, this must be logged through the Information Governance Data Security and Protection Toolkit by the IG Team.

16.3 All information incidents must be reported to the Information Governance team who will work with staff to understand the severity of the incident and determine whether external reporting is required.

16.4 Upon receipt of adequate information, the Head of Information Governance/ Data Protection Officer will make an initial assessment and notify the Director of Corporate Affairs, the SIRO and any other senior management as necessary.

16.5 A full investigation will commence dependent on the situation which will be agreed by senior management/ executive leads at the time and an investigation lead will be assigned.

16.6 The Head of Information Governance/ DPO is the lead contact for the Supervisory Authority (ICO) and will manage contact and correspondence to resolve any issues to support and to the point of their decision in line with ICB senior management.

17. Equality and Diversity Statement

17.1. NHS Nottingham and Nottinghamshire ICB pays due regard to the requirements of the Public Sector Equality Duty (PSED) of the Equality Act 2010 in policy development and implementation, as a commissioner and provider of services, as well as an employer.

17.2. The ICB is committed to ensuring that the way we provide services to the public and the experiences of our staff does not discriminate against any individuals or groups on the basis of their age, disability, gender identity (trans, non-binary), marriage or civil partnership status, pregnancy or maternity, race, religion or belief, gender or sexual orientation.

17.3. We are committed to ensuring that our activities also consider the disadvantages that some people in our diverse population experience when accessing health services. Such disadvantaged groups include people experiencing economic and social deprivation, carers, refugees and asylum seekers, people who are homeless, workers in stigmatised occupations, people who are geographically isolated, gypsies, Roma and travellers.

17.4. As an employer, we are committed to promoting equality of opportunity in recruitment, training and career progression and to valuing and increasing diversity within our workforce.

17.5. To help ensure that these commitments are embedded in our day-to-day working practices, an Equality Impact Assessment has been completed for, and is attached to, this policy.

18. Communication, Monitoring and Review

18.1 Information on incident reporting will be provided as part of the organisation's induction process.

18.2 The Head of Corporate Assurance and Head of Information Governance will be responsible for monitoring the use of this policy on an ongoing basis.

18.3 Reporting on corporate incidents will form part of the Work Programmes of the Information Governance Steering Group and Health, Safety and Security Steering Group. Formal reporting will occur twice yearly to the Audit and Risk Committee and annually to the Integrated Care Board. This policy will be reviewed by the Health, Safety and Security Steering Group and Information Governance Steering Group every three years or following any legislative changes.

18.4 The Equality Impact Analysis will also be reviewed in light of any necessary changes to the policy, where this might be performed sooner than the required review date.

18.5 Any individual who has queries regarding the content of this policy, or has difficulty understanding how this policy relates to their role, should contact the Head of Corporate Assurance via email at nnicb-nn.corporateassurance2@nhs.net .

19. Staff Training

19.1 The Corporate Assurance Team will proactively raise awareness of the Policy across the ICB and provide ongoing support to committees and individuals to enable them to discharge their responsibilities. Members of the Corporate Assurance Team/Information Governance Team can be contacted for formal training at team meetings (or other forums) by email at nnicb-nn.corporateassurance2@nhs.net or nnicb-nn.igteam@nhs.net.

19.2 Any individual who has queries regarding the content of the Policy, or has difficulty understanding how this relates to their role, should contact the Head of Corporate Assurance or Head of Information Governance dependent on the nature of their query.

20. Interaction with other Policies

20.1. This policy should be read in conjunction with the following ICB policies:

- Information Security Policy;
- Data Protection and Confidentiality Policy;
- Health and Safety (and Security) Policy;
- Standards of Business Conduct Policy.

21. References

- Data Security (2020) Data Security Toolkit reporting requirements
- Health and Safety Executive (2012) Reporting accidents and incidents at work
- Health and Social Care Information Centre / NHS Digital
- (2018) Guide to the Notification of Data Security and Protection Incidents (SIRI Guide 2018)

22. Equality Impact Assessment

Overall Impact on Equality, Inclusion and Human Rights [Select one option]	**Neutral**
Policy	**Incident Reporting and Management Policy**

	What are **the actual, expected or potential positive impacts** of the policy, process, strategy or service change?	What are the **actual, expected or potential negative impacts** of the policy, process, strategy or service change?	What **actions have been taken** to address the actual or potential **positive and negative impacts** of the policy, process, strategy or service change?	**Impact Score**
Age	There are no actual or expected positive impacts on the characteristic of Age.	There are no actual or expected negative impacts on the characteristic of Age.	None.	3
Disability[1] (Including: mental, physical, learning, intellectual and neurodivergent)	There are no actual or expected positive impacts on the characteristic of Disability.	There are no actual or expected negative impacts on the characteristic of Disability.	Mechanisms are in place via the Communications and Engagement Team to receive the policy in a range of languages, large print, Braille, audio, electronic and other accessible formats.	3

Gender[2] (Including: trans, non-binary and gender reassignment)	There are no actual or expected positive impacts on the characteristic of Gender.	There are no actual or expected negative impacts on the characteristic of Gender.	None.	3
Marriage and Civil Partnership	There are no actual or expected positive impacts on the characteristic of Marriage and Civil Partnership.	There are no actual or expected negative impacts on the characteristic of Marriage and Civil Partnership.	None.	3
Pregnancy and Maternity Status	There are no actual or expected positive impacts on the characteristic of Pregnancy and Maternity Status.	There are no actual or expected negative impacts on the characteristic of Pregnancy and Maternity Status.	None.	3
Race[3]	There are no actual or expected positive impacts on the characteristic of Race.	There are no actual or expected negative impacts on the characteristic of Race.	None.	3
Religion and Belief[4]	There are no actual or expected positive impacts on the characteristic of Religion or Belief.	There are no actual or expected negative impacts on the characteristic of Religion or Belief.	None.	3
Sex[5]	There are no actual or expected positive impacts on the characteristic of Sex.	There are no actual or expected negative impacts on the characteristic of Sex.	None.	3

Sexual Orientation[6]	There are no actual or expected positive impacts on the characteristic of Sexual Orientation.	There are no actual or expected negative impacts on the characteristic of Sexual Orientation.	None.	3
Human Rights[7]	There are no actual or expected positive impacts on the characteristic of Human Rights.	There are no actual or expected negative impacts on the characteristic of Human Rights.	None.	3
Community Cohesion and **Social Inclusion**[8]	There are no actual or expected positive impacts on the characteristic of Community Cohesion and Social Inclusion.	There are no actual or expected negative impacts on the characteristic of Community Cohesion and Social Inclusion.	None.	3
Safeguarding[9] (Including: adults, children, Looked After Children and adults at risk or who lack capacity)	There are no actual or expected positive impacts on the characteristic of Safeguarding.	There are no actual or expected negative impacts on the characteristic of Safeguarding.	None.	3
Other Groups at Risk[10] of Stigmatisation, Discrimination or Disadvantage	There are no actual or expected positive impacts on the characteristic of Other Groups at Risk.	There are no actual or expected negative impacts on the characteristic of Other Groups at Risk.	None.	3

1. **Disability** refers to anyone who has: "…a physical or mental impairment that has a 'substantial' and 'long-term' negative effect on your ability to do normal daily activities…" (Equality Act 2010 definition). This includes, but is not limited to: mental health conditions, learning disabilities, intellectual disabilities, neurodivergent conditions (such as dyslexia, dyspraxia and dyscalculia), autism, many physical conditions (including HIV, AIDS and cancer), and communication difficulties (including d/Deaf and blind people).

2. **Gender**, in terms of a Protected Characteristic within the Equality Act 2010, refers to: "A person has the protected characteristic of gender reassignment if the person is proposing to undergo, is undergoing or has undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attributes of sex."

3. **Race**, in terms of a Protected Characteristic within the Equality Act 2010, refers to: A person's colour, nationality, or ethnic or national origins. This also includes people whose first spoken language is not English, and/or those who have a limited understanding of written and spoken English due to English not being their first language.

4. **Religion and Belief**, in terms of a Protected Characteristic within the Equality Act 2010, refers to: Religion means any religion and a reference to religion includes a reference to a lack of religion. Belief means any religious or philosophical belief and a reference to belief includes a reference to a lack of belief.

5. **Sex**, in terms of a Protected Characteristic within the Equality Act 2010, refers to: A reference to a person who has a particular protected characteristic and is a reference to a man or to a woman.

6. **Sexual Orientation**, in terms of a Protected Characteristic within the Equality Act 2010, refers to: Sexual orientation means a person's sexual orientation towards persons of the same sex, persons of the opposite sex or persons of either sex.

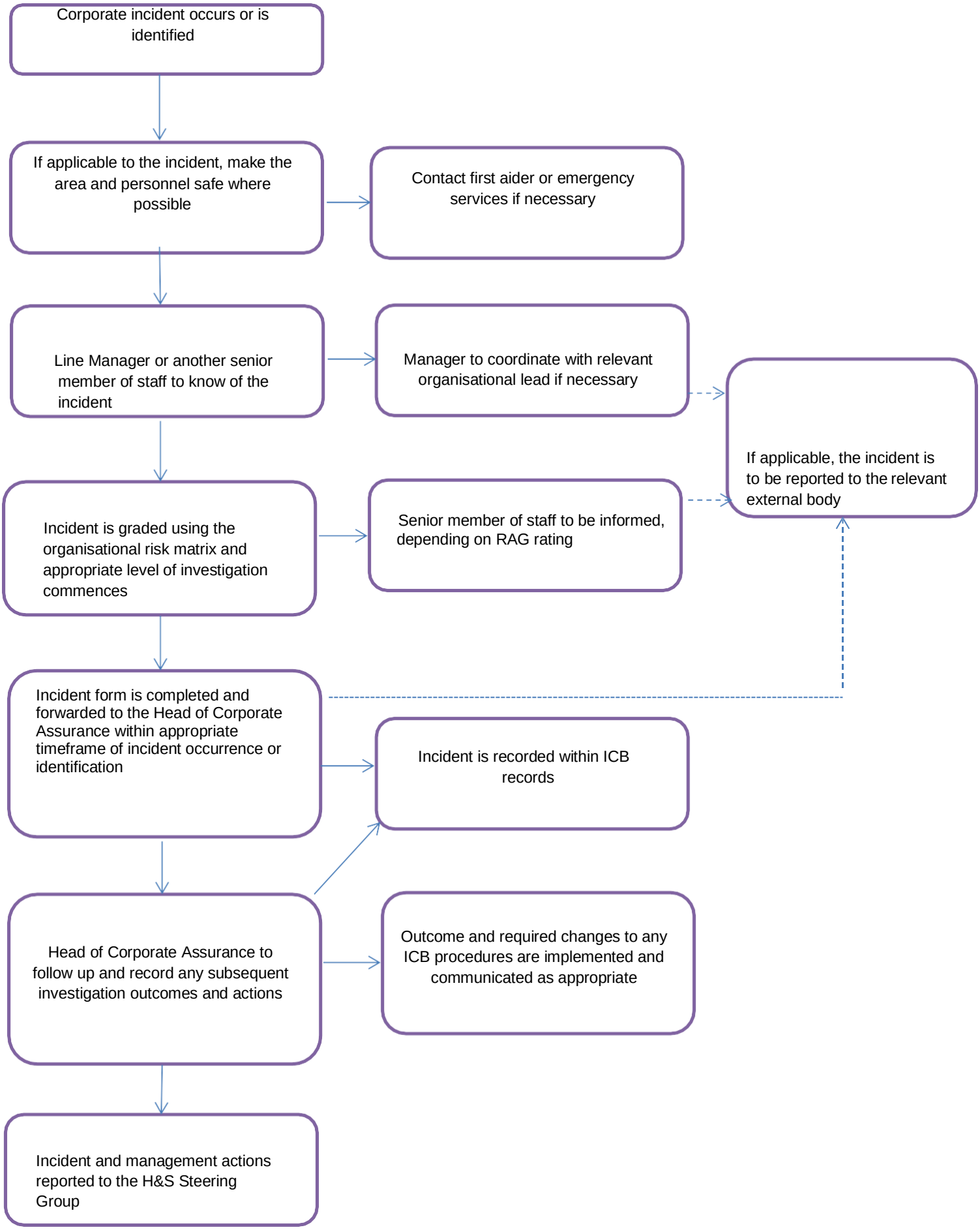
7. The **Human Rights Act 1998** sets out the fundamental areas that everyone and every organisation must adhere to. In relation to health and care, the most commonly applicable of the Articles within the Human Rights Act 1998 include: Article 2 Right to Life, Article 5 Right to Liberty and Security, Article 8 Right to Respect of Private and Family Life, and Article 9 Freedom of Thought, Conscience and Religion.

8. **Community Cohesion** is having a shared sense of belonging for all groups in society. It relies on criteria such as: the presence of a shared vision, inclusion of those with diverse backgrounds, equal opportunity, and supportive relationships between individuals. **Social Inclusion** is defined as the process of improving the terms of participation in society, particularly for people who are disadvantaged, through enhancing opportunities, access to resources, voice and respect for rights (United Nations definition). For the EQIA process, we should note any positive or negative impacts on certain groups being excluded or not included within a community or societal area. For example, people who are homeless, those from different socioeconomic groups, people of colour or those from certain age groups.

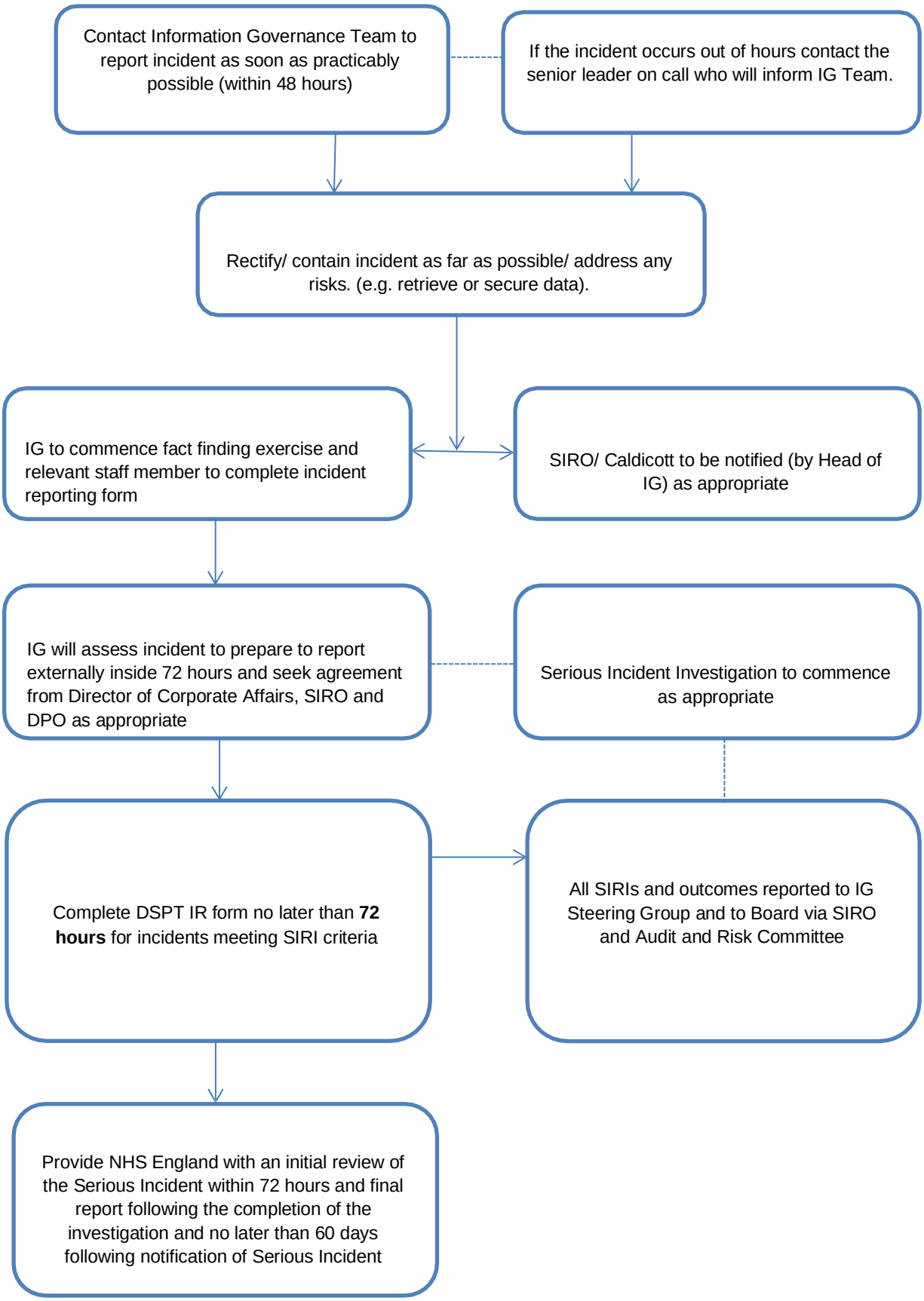
9. **Safeguarding** means: "…protecting a citizen's health, wellbeing and human rights; enabling them to live free from harm, abuse and neglect. It is an integral part of providing high-quality health care. Safeguarding children, young people and adults is a collective responsibility" (NHS England definition). Those most in need of protection are children, looked after children, and adults at risk (such as those receiving care, those under a DoLS or LPS Order, and those with a mental, intellectual or physical disability). In addition to the ten types of abuse set out in the Health and Care Act 2022, this section of the EQIA should also consider PREVENT, radicalisation and counterterrorism.

10. **Other Groups** refers to anyone else that could be positively or negatively impacted by the policy, process, strategy or service change. This could include, but is not limited to: carers, refugees and asylum seekers, people who are homeless, gypsy, Roma and traveller communities, people living with an addiction (e.g., alcohol, drugs or gambling), people experiencing social or economic deprivation, and people in stigmatised occupations (e.g., sex workers).

Appendix A: Incident Reporting and Management Process (for non-IG incidents)



Appendix B: Incident Reporting and Management Process (for IG incidents (e.g. reporting data breaches))



Appendix C: Incident Grading: Risk Assessment

Matrix Table 1 – Impact Scores

What is the potential severity of the *impact?*					
Impact Score	**1**	**2**	**3**	**4**	**5**
Descriptor	**Insignificant or minor**	**Moderate**	**Significant**	**Very significant**	**Major**

Table 2 – Likelihood Scores

What is the *likelihood* that harm, loss or damage from the incident will reoccur?					
Likelihood Score	**1**	**2**	**3**	**4**	**5**
Descriptor	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost Certain**

When the impact and likelihood of a risk has been evaluated, Table 3 should be used to determine a 'RAG' rating for the risk. This will influence the level of investigation required.

Table 3 – RAG rating

Impact	5 - Major /	5	10	15	20	25
	4 - Very Significant	4	8	12	16	20
	3 - Significant	3	6	9	12	15
	2 - Moderate	2	4	6	8	10
	1 - Insignificant /	1	2	3	4	5
		1 - Rare	2 - Unlikely	3 - Possible	4 - Likely	5 - Almost Certain
		Likelihood				

Guidance on Incident Investigation

The ‘RAG’ rating will determine the level of investigation required. Whilst not all incidents will require a comprehensive investigation, it is essential that all incidents receive adequate review to ensure that lessons are learnt and reoccurrence prevented.

All incidents will be reported to the Audit and Risk Committee to provide assurance that any associated risks have been adequately addressed; however, the grading of the incident will reflect the timescale of this and the detail required.

The amount of investigative effort should relate to whether the incident resulted in harm and / or if it is likely to recur. For incidents where a comprehensive investigation needs to be undertaken, it is important that the right people are involved. This could be another member of staff, or an independent investigator.

A casual approach should be taken towards the investigation of any incident. The focus should be on systems and processes rather than any individuals involved, which may have led to the incident occurring.

As a guide, all investigations should generally consist of the following activities:

- **Data gathering** - e.g. written statements, records, relevant policies/procedures etc.
- **Information mapping** - e.g. the timeline of events, who was involved etc.
- **Identifying problems** - e.g. where and when processes went wrong.
- **Analysing problems for contributory factors** - factors which may have had an effect on the incident, e.g. communication factors, training factors, etc.
- **Agreeing the root causes** - the fundamental issue that led to the incident occurring.
- **Recommendations and reporting** – all investigations should result in recommendations and actions that will mitigate the possibility of recurrence.

Interviewing anyone involved in the incident may be a critical part of the investigation process. Interviewers should be aware of the need to elicit information effectively and sensitively from people.

All incidents are different; however, the following should be used as a guide to the level of investigation required and the members of ICB staff who should be informed:

	Red Incidents	Red/Amber Incidents	Amber Incidents	Amber/Green Incidents	Green Incidents
Level of Investigation	This category of Incidents must be addressed immediately and subject to a comprehensive investigation.	This category of incidents must be addressed immediately and subject to a comprehensive investigation.	This category of incidents must be addressed immediately and subject to a comprehensive investigation.	These incidents should be subject to review and discussion by appropriate personnel.	These incidents are considered as 'low Level' however, appropriate review and discussion are required.
Who should be informed?	A member of the Executive Management Team should be informed immediately.	The relevant Assistant Director should be informed immediately and a member of the Executive Management Team as soon as possible.	The relevant Assistant Director should be informed immediately.	These incidents should be subject to review and discussion by appropriate personnel.	Incidents at this level can be dealt with at team level and overseen by the Line Manager.
Outcome reporting and assurance	The full details of Incidents in this category will be reported to the Audit and Risk Committee, along with the subsequent investigation results.	The full details of Incidents in this category will be reported to the Audit and Risk Committee, along with the subsequent investigation results.	A summary of incidents in this category will be reported to the Audit and Risk Committee on a biannual basis.	A summary of incidents in this category will be reported to the Audit and Risk Committee on a biannual basis.	A summary of incidents in this category will be reported to the Audit and Risk Committee on a biannual basis.

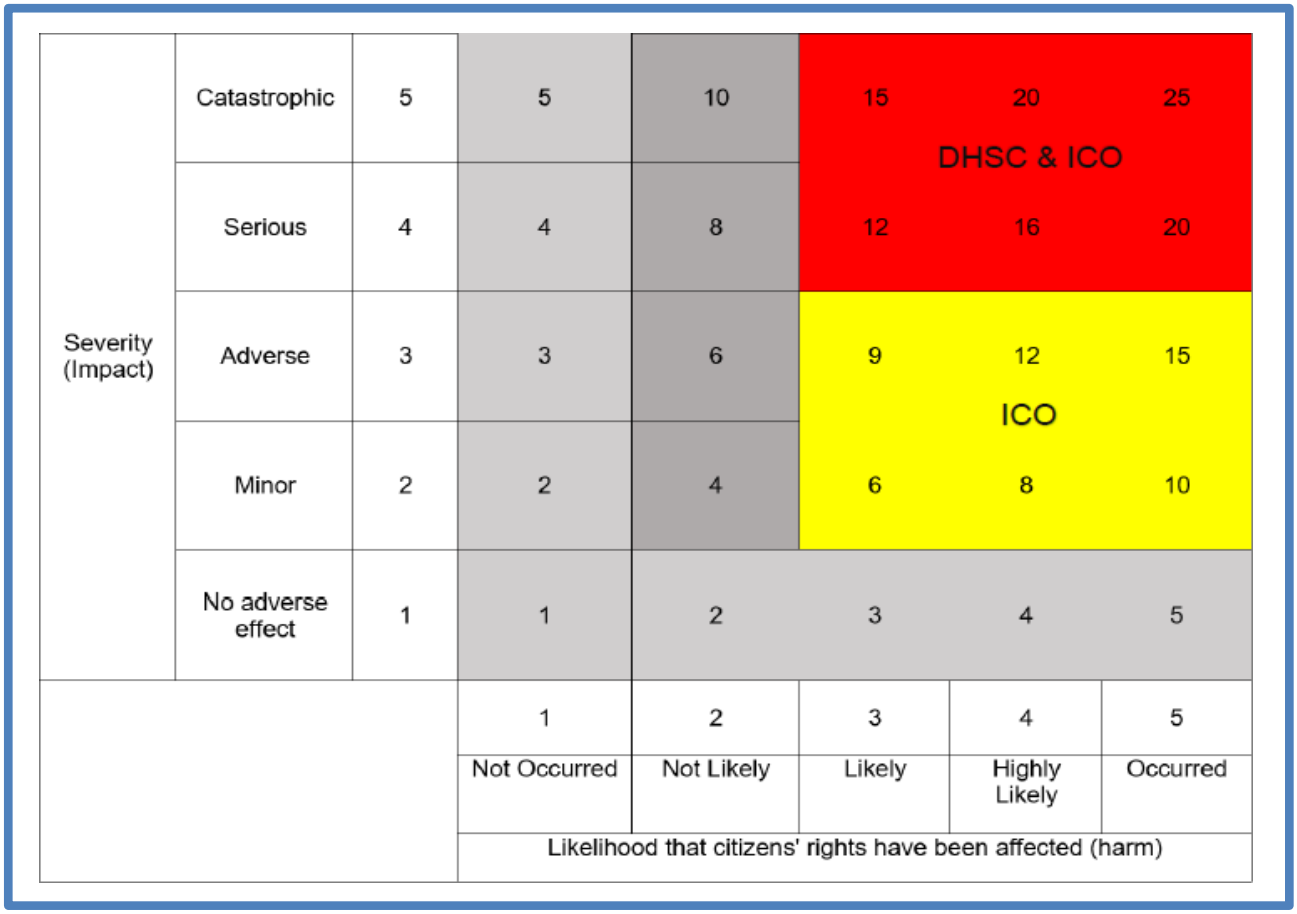
Appendix D: Severity Tables Likelihood – (DSPT IR SIRI Guide)

No.	Likelihood	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

Impact (severity of adverse impact on the affected individual(s))

No.	Effect	Description
1	No adverse effect	There is absolute certainty that there can be no adverse effect arising from the breach.
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.
3	Potentially some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.
4	Potentially Pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5	Death/ catastrophic event	A person dies or suffers a catastrophic occurrence

Severity Score Matrix for IG breaches



Appendix E: Information Governance Incident Report Form

Part 1 to be completed as soon as possible for all Information Governance (IG) Information Security, Cyber Security Incidents or Near Misses as set out in Section 9 of the Incident Reporting and Management Policy and returned to Information Governance Team at:nnicb-nn.igteam@nhs.net. **Part 2** to be completed by manager following Individuals completing this form can request guidance from the IG Team. **Part 3** to be completed by the IG Team.

<table>
<tr><th colspan="2">Incident Details – Part 1</th></tr>
<tr><td>☐ Incident/Breach
☐ Near Miss</td><td>Type of Incident:
☐ Confidentiality
☐ Integrity
☐ Availability</td></tr>
<tr><td>Reported by (Name):
Job Title:
Team/Service:
Directorate:
Email:
Telephone Number:</td><td>Location of Incident:
Team/Service:
Team Manager:
Directorate:
Director:</td></tr>
<tr><td>Date Incident/ Breach or Near Miss Occurred:
Time:</td><td>Date Incident/Breach or Near Miss Reported:
Reasons for delay in reporting (if applicable):</td></tr>
<tr><td colspan="2">How was the incident/breach or near miss initially identified/ notified and when?</td></tr>
<tr><td colspan="2">Incident Category:
☐ Accidental destruction, loss, or alteration
☐ Accidental disclosure
☐ Cyber incident
☐ Inappropriate access
☐ Inappropriate access controls allowing unauthorised access and/or use
☐ Failure, loss or theft of data, equipment or device on which personal data is stored
☐ Offences where information is obtained by deceiving the holder of the information
☐ Unauthorised access or disclosure
☐ Unforeseen circumstances i.e. fire/flood etc
☐ Unlawful destruction, loss, alteration or disclosure</td></tr>
</table>

Brief description of incident/ breach (fuller description required below): ***NOTE Please do NOT identify any individuals involved. Describe generically.**	
What is the information? List all the data fields e.g., NHS number, First name, surname, D.O.B.	
Has this impacted the Team/Service/Department (total failure, business as usual affected etc.):	**Type of affected Information System (E.g., name of system/email/paper/electronic):**
How many individuals is the information about? (If not known give approximate or highest possible number)	
How many records are involved? (if not known give approximate or highest possible number)	
What security controls were in place? (E.g., was the information encrypted? sent via secure email?)	
Full factual description of the incident: (include times and dates). If applicable include details about any vulnerable groups and of any other organisations involved and the ICB's relationship with that organisation e.g., we hold a current contract with them.	
Immediate Actions Taken:	
Root Cause of incident:	
Contributory Factors Identified:	
Staff mandatory Annual Data Security and Protection/IG training at the time of incident: Completed: YES ☐ NO ☐ Date Achieved:	
Have the affected individuals (whose personal data has been breached) been informed? YES ☐ NO ☐ **If YES - please provide the IG Team with the full details separately.** **If NO - please provide the reason for that decision:**	

Incident Details – Part 2 (Investigation Outcome)

(To be completed following investigation – within 28 days following Part 1 Incident Report)

Reference No (provided by IG Team):	
Date:	

Nottingham & Nottinghamshire ICB ('the ICB) are required to have robust objectives and controls in place for preventing data breaches and for managing them in the rare event that they do occur.

Due to the nature of our business, the ICB process and stores personal data, special category personal data and confidential data and as such, have developed a structured and documented breach incident program to mitigate the impact of any data breaches and to ensure that the correct notifications are made.

Investigations by managers of data breaches should identify gaps in business processes that caused/contributed to the breach which should be risk assessed and revised and to mitigate any future occurrence of the same root cause.

As part of this data breach review please confirm that the investigation considered:

1. Where and how personal data involved in the breach was held;
2. Where and how it was stored;
3. Where and how it was transmitted;
4. Whether methods of transmission were secure; and that there was only sharing of minimum amount of data necessary;
5. The classification of personal and special category data and sensitivity of the data involved in the breach;
6. The investigation identified the weak points within existing business area personal data processing that led to the breach;
7. The number of individuals whose personal data was affected by the incident, and where it was considered likely to result in a high risk of adversely affecting that individual's rights and freedoms under data protection legislation, they were informed without undue delay.
8. Implementation of a data breach plan to address the weak points by identifying responsibility for reacting to the breach, investigating and making changes to business personal data handling processes that addressed the identified gaps to mitigate any future occurrence.
9. As a result of the investigation awareness was raised with staff of the Staff IG Handbook, ICB IG Policies, Data Security Training and the requirement to only use ICB approved policies, procedures and devices when handling personal data.

Lessons Learned: (what actions have been implemented to reduce the likelihood of the incident happening again?)

Manager Name	Job Title	Signature
Date:		

Incident Details – Part 3 (IG Team Risk Assessment & Reporting)

Risk grading BEFORE any further action is taken (based on the NHS Digital "Guide to the Notification of Data Security and Protection Incidents" SIRI Guide 2018):

Risk grading after investigation and actions undertaken

Impact: 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

Likelihood: 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

Total score =

Informed/ date:	**Informed/ date:**
IG Team:	SIRO:
DPO:	Caldicott Guardian:
IAO:	Director(s):

Details of investigation, actions and outcome

Full investigation completed?: Yes/ No	**Externally Reported:** YES ☐ NO ☐ **(Date or N/A):**
Completed by:	**Designation:**

Risk grading AFTER investigation and actions undertaken

Impact: 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

Likelihood: 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

Total score =

Please detail any lessons that have been learned and how these have been shared (for instance staff meetings, email, in person)

Updates provided to date: SIRO: Caldicott Guardian: Associate Director(s): DPO:	

Please return Part 1 as soon as possible and Part 2 following investigation to the IG Team (email: nnicb-nn.igteam@nhs.net).

The IG Team to forward this form to Corporate Assurance Team upon completion and review (nnicb-nn.corporateassurance2@nhs.net).