

Incident Reporting and Management Policy¹

July 2022 - July 2024

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

| CONTROL RECORD | | | |
|--|---|------------------------|---|
| Reference Number GOV-019 | Version 1.2 | Status Final | Author Head of Corporate Assurance; Head of Information Governance |
| | | | Sponsor Associate Director of Governance |
| | | | Team Corporate Assurance; Information Governance |
| Title | Incident Reporting and Management Policy | | |
| Amendments | Email address update in Appendix F | | |
| Purpose | <p>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.</p> <p>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).</p> | | |
| Superseded Documents | Incident Reporting and Management Policy v1.1 | | |
| 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 – June 2022 | | |
| Approving Body | ICB Board | Date approved | 1 July 2022 |
| Date of Issue | July 2022 | | |
| Review Date | July 2024 | | |
| <p>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.</p> | | | |

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

| | Page |
|---|-------------|
| 1 Introduction | 5 |
| 2 Purpose | 5 |
| 3 Scope | 5 |
| 4 Definitions | 6 |
| 5 Roles and Responsibilities | 6 |
| 6 Fair Blame | 8 |
| 7 Reporting Incidents | 8 |
| 8 Initial Management of the Incident | 9 |
| 9 Information Governance Incidents: Personal Data Breaches | 9 |
| 10 External Stakeholder Notification | 10 |
| 11 Incident Grading | 11 |
| 12 Incident Investigation | 11 |
| 13 Learning from Incidents | 12 |
| 14 Media Involvement | 12 |
| 15 Serious Incidents | 12 |
| 16 Equality and Diversity Statement | 14 |
| 17 Communication, Monitoring and Review | 14 |
| 18 Staff Training | 15 |
| 19 Interaction with other Policies | 15 |
| 20 References | 15 |
| 21 Equality Impact Assessment | 16 |
| APPENDICES: | |
| Appendix A: Incident Reporting and Management Process (for non-IG incidents) | 18 |
| Appendix B: Incident Reporting and Management Process (for IG incidents) | 19 |
| Appendix C: Incident Grading: Risk Assessment Matrix; and Guidance on Incident Investigation | 20 |

| | |
|---|----|
| Appendix D: Severity Tables Likelihood (DSPT IR SIRI Guide) | 23 |
| Appendix E: Incident Report Form (non-IG) - Part 1 | 25 |
| Appendix F: Incident Report Form for Data Breaches (IG) - Part 1 | 27 |
| Appendix G: Incident Report Form - Part 2 | 30 |

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.
 - 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 | <p>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:</p> <ul style="list-style-type: none">• Information governance (e.g. the unauthorised or inappropriate disclosure of person identifiable data or the loss of unencrypted IT equipment).• 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). |
| Accident | <p>An accident is an unplanned or unexpected event that resulted in, or could have resulted in, injury or harm to staff or visitor.</p> |
| Near miss | <p>A near miss can be described as an event where one of the above almost occurred or had the potential to occur.</p> |

5. Roles and Responsibilities

| Role | Responsibilities |
|---------------------------------|---|
| Integrated Care Board | <p>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.</p> |
| Audit and Risk Committee | <p>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.</p> |

| 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. |
| 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 | <p>Has a responsibility to ensure that:</p> <ul style="list-style-type: none"> • 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 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. |

| Role | Responsibilities |
|------------------|--|
| All Staff | Have a responsibility for: <ul style="list-style-type: none"> • 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 retribution.
- 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 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 an 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 Specific reporting requirements in relation to an information governance, or personal data breach, are provided at **Appendix B** of this policy.
- 7.4 The person involved in the incident or who has identified the incident should complete the Incident Report Form - Part 1 (**Appendix E**). 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.
- 7.5 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: notts.corporateassurance@nhs.net). Incidents relating to Information Governance should also be copied into the IG Team via nnicb-nn.igteam@nhs.net.

- 7.6 The Incident Report Form – Part 1 should record factual details of the incident and details of any immediate actions taken. **Appendix E** is for all incidents other than those relating to Information Governance, for which **Appendix F** should be completed.
- 7.7 The Head of Corporate Assurance and/or 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.
- 7.8 The investigation outcome needs to be detailed on the Incident Report Form – Part 2 (**Appendix G**), along with any lessons learned and how these have been shared.
- 7.9 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 \(RIDDOR\)](#).
- 7.10 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. ***This does not apply to Information Governance incidents, which are led by the organisation's SIRO.***
- 7.11 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.

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 appropriate incident report (**Appendix F**).
- 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.

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 Associate Director of Governance, 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.

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.

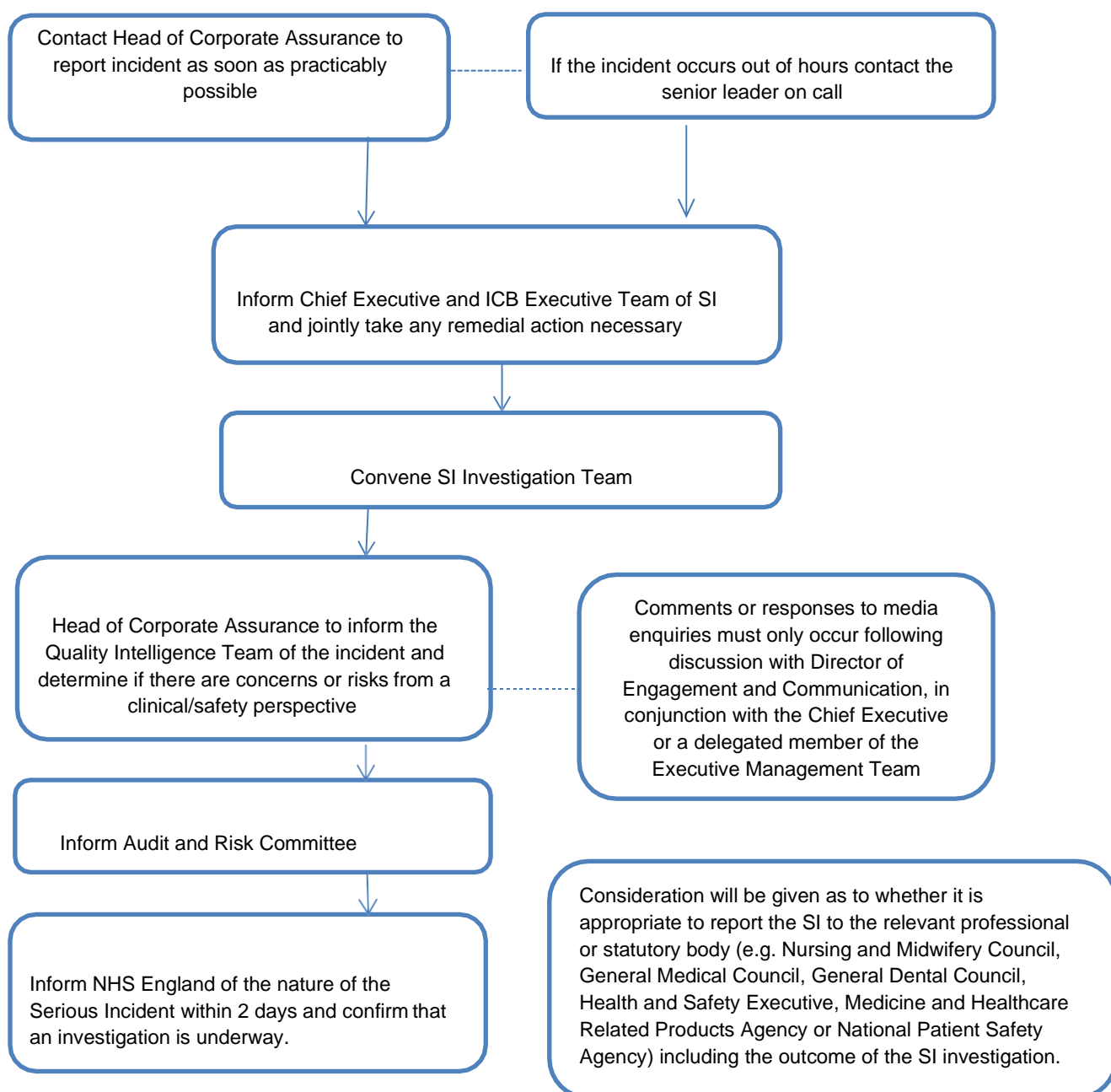
14. Media Involvement

- 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

- 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 outlines the process to follow when reporting an SI:



- 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.

16. Equality and Diversity Statement

- 16.1. 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.
- 16.2. 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.
- 16.3. 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.
- 16.4. 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.
- 16.5. 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.

17. Communication, Monitoring and Review

- 17.1 Information on incident reporting will be provided as part of the organisation's induction process.
- 17.2 The Head of Corporate Assurance and Head of Information Governance will be responsible for monitoring the use of this policy on an ongoing basis.
- 17.3 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.

17.4 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.

17.5 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 – notts.corporateassurance@nhs.net.

18. Staff Training

18.1 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: notts.corporateassurance@nhs.net or nnicb-nn.igteam@nhs.net.

18.2 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.

19. Interaction with other Policies

19.1. 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.

20. 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)

21. Equality Impact Assessment

| Date of assessment: | June 2022 | | | |
|---|---|---|--|--|
| For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups: | Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity? | If yes, are there any mechanisms already in place to mitigate the adverse impacts identified? | Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned. | Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe. |
| Age ² | No | N/A | N/A | This policy is aimed at all staff and they should follow the procedures set out in the policy to enable them to work in a safe and secure environment. |
| Disability ³ | No | N/A | N/A | |
| Gender identity (trans, non-binary) ⁴ | No | N/A | N/A | |
| Marriage or civil partnership status ⁵ | No | N/A | N/A | |
| Pregnancy or maternity ⁶ | No | N/A | N/A | |
| Race ⁷ | No | N/A | N/A | |

² A person belonging to a particular age (for example 32 year olds) or range of ages (for example 18 to 30 year olds).

³ A person has a disability if she or he has a physical or mental impairment which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities.

⁴ The process of transitioning from one gender to another.

⁵ Marriage is a union between a man and a woman or between a same-sex couple.

Same-sex couples can also have their relationships legally recognised as 'civil partnerships'.

⁶ Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth, and is linked to maternity leave in the employment context. In the non-work context, protection against maternity discrimination is for 26 weeks after giving birth, and this includes treating a woman unfavourably because she is breastfeeding.

⁷ Refers to the protected characteristic of race. It refers to a group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins.

| | | | | |
|--|---|---|--|---|
| Date of assessment: | June 2022 | | | |
| For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups: | Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity? | If yes, are there any mechanisms already in place to mitigate the adverse impacts identified? | Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned. | Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe. |
| Religion or belief⁸ | No | N/A | N/A | |
| Gender⁹ | No | N/A | N/A | |
| Sexual orientation¹⁰ | No | N/A | N/A | |
| Carers¹¹ | No | N/A | N/A | |

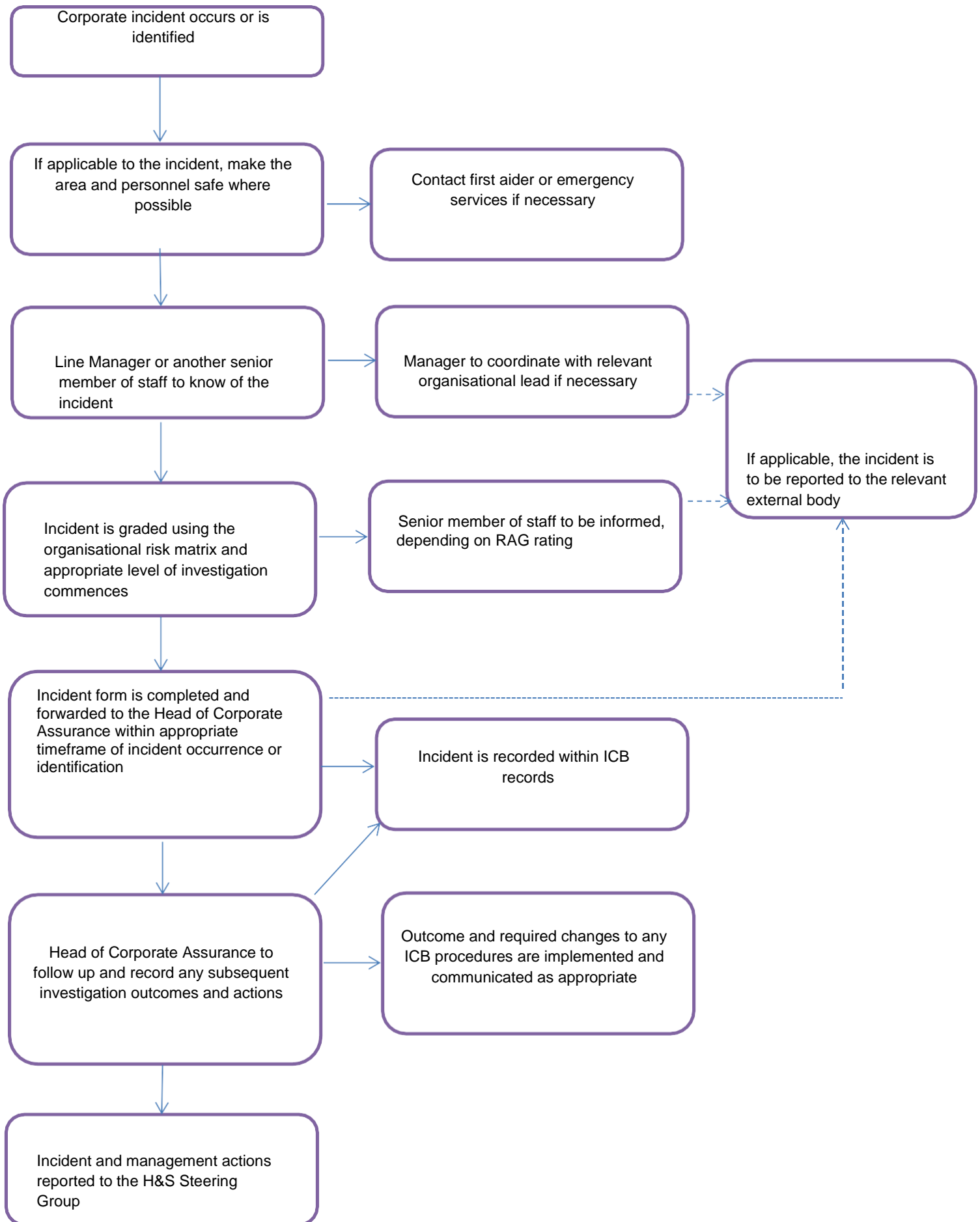
⁸ Religion refers to any religion, including a lack of religion. Belief refers to any religious or philosophical belief and includes a lack of belief. Generally, a belief should affect your life choices or the way you live for it to be included in the definition.

⁹ A man or a woman.

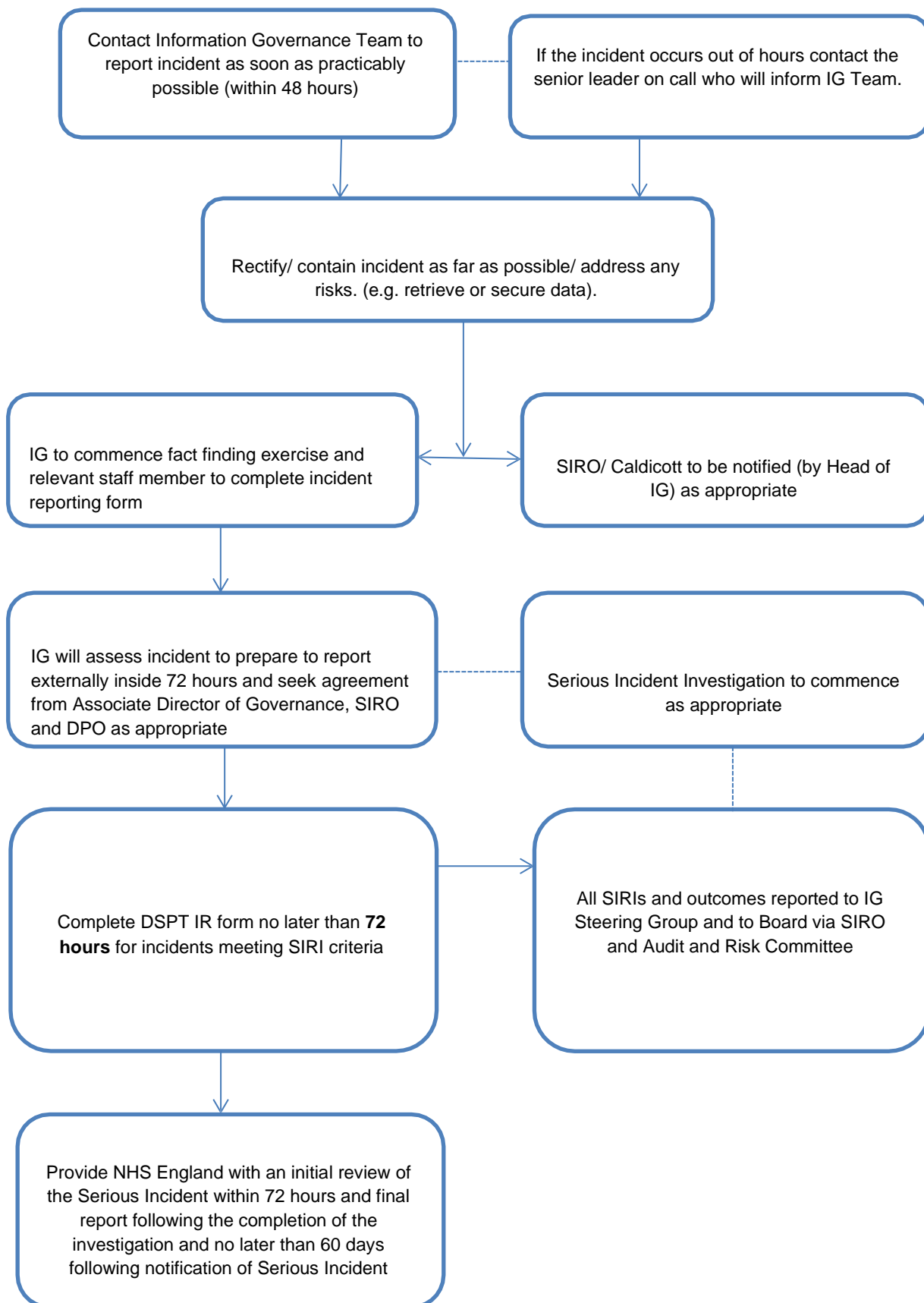
¹⁰ Whether a person's sexual attraction is towards their own sex, the opposite sex, to both sexes or none. <https://www.equalityhumanrights.com/en/equality-act/protected-characteristics>

¹¹ Individuals within the ICB which may have carer responsibilities.

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 <i>impact</i> ? | | | | | |
|---|------------------------|----------|-------------|------------------|-------|
| Impact Score | 1 | 2 | 3 | 4 | 5 |
| Descriptor | Insignificant or minor | Moderate | Significant | Very significant | Major |

Table 2 – Likelihood Scores

| What is the <i>likelihood</i> 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

| | | | | | | | |
|----------------------|-------------------|---|--|------------|----------------------------------|---------------|----------|
| Severity (Impact) | Catastrophic | 5 | 5 | 10 | 15 20 25 DHSC & ICO | | |
| | Serious | 4 | 4 | 8 | 12 16 20 | | |
| | Adverse | 3 | 3 | 6 | 9 12 15 ICO | | |
| | Minor | 2 | 2 | 4 | 6 8 10 | | |
| | No adverse effect | 1 | 1 | 2 | 3 | 4 | 5 |
| | | | 1 | 2 | 3 | 4 | 5 |
| | | | Not Occurred | Not Likely | Likely | Highly Likely | Occurred |
| | | | Likelihood that citizens' rights have been affected (harm) | | | | |

Appendix E: Incident Report Form (non-IG) - Part 1

Incident Report Form (non-IG)

(for all incidents other than those relating to Information Governance)

Please return to the Corporate Assurance Team notts.corporateassurance@nhs.net

| Details of the accident, incident or near miss | |
|--|--|
| Incident Type: | Accident <input type="checkbox"/> Incident <input type="checkbox"/> Near Miss <input type="checkbox"/> |
| Date: | [DD/MM/YYYY] |
| Time: | |
| Location: | ICB Base <input type="checkbox"/> Home <input type="checkbox"/> Provider Organisation <input type="checkbox"/> <i>Please add further detail if required</i> |

| Details of the person affected | |
|--------------------------------|--|
| Name: | |
| Job Title: | |
| Line Manager Name: | |
| Directorate: | |
| Team: | |
| Contact Number: | |
| Names of any witnesses: | |

| | |
|---|--------------------------|
| Details of incident | |
| Factual description of incident: | |
| | |
| Details of immediate action taken: | |
| | |
| Details of any injury: | |
| | |
| Details of treatment received and any subsequent absence: | |
| None | <input type="checkbox"/> |
| First Aider | <input type="checkbox"/> |
| Emergency Services | <input type="checkbox"/> |
| GP | <input type="checkbox"/> |
| Details of any planned actions: e.g. awareness raising, new procedure to be put in place, training, repair of any faulty equipment etc | |
| | |
| Confirm if further investigation is required? | |
| Yes | <input type="checkbox"/> |
| No | <input type="checkbox"/> |

| | | | | | |
|--|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Risk grading BEFORE any further action is taken | | | | | |
| Impact: | 1 | 2 | 3 | 4 | 5 |
| | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Likelihood: | 1 | 2 | 3 | 4 | 5 |
| | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Please return to the Corporate Assurance Team notts.corporateassurance@nhs.net

Appendix F: Incident Report Form for Data Breaches (IG) – Part 1

Information Governance Incident Report Form

To be completed for all Information Governance (IG) Information Security, Cyber Security Incidents or Near Misses **and returned to** the Information Governance Team nnicb-nn.igteam@nhs.net

| Incident Details | |
|---|--|
| Incident <input type="checkbox"/> Near Miss <input type="checkbox"/> | Type of Incident: Confidentiality <input type="checkbox"/> Integrity <input type="checkbox"/> Availability <input type="checkbox"/> |
| Date Incident Occurred: Time: | Location of Incident: |
| Date Reported: Reasons for delay in reporting (if applicable): | Reported by (Name): Title: Email: Telephone Number: |
| Incident Category: <ul style="list-style-type: none"> • Data Loss / Theft / Unavailability • Inappropriate / unauthorised disclosure • Cyber incident | |
| Brief description of incident / breach (fuller description required below): | |
| What is the information? List all the data fields e.g. NHS number, First name, surname, D.O.B. | |

| | |
|---|---------------------------------|
| Impacts on the Department (total failure, business as usual etc.): | Type of affected System: |
| 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: | |

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):

Likelihood:

Consequence:

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

IG Team Use

IG SIRI Level:

Likelihood of adverse effect:

Severity of adverse effect:

Total score =

Informed/ date:

SIRO:

Caldicott Guardian:

Associate Director(s):

DPO:

Full investigation completed?: Yes / No

Externally Reported: (Date or N/A)

