Note to staff (18/03/2020):
Until the Incident module is running on Datix, staff are asked to report incidents in the interim as follows:

- **Information Governance incidents**: gwccg.informationgovernance@nhs.net.
- **All other incidents**: report to the Senior Business Support and Facilities Manager (based at NWS)

Staff should direct any queries on this policy to: sdccg.governance.surreyheartlands@nhs.net

CORP08

Incident Reporting and Management Policy

Policy applicable to:

NHS East Surrey CCG	✓
NHS Guildford and Waverley CCG	✓
NHS North West Surrey CCG	✓
NHS Surrey Downs CCG	✓

The above four CCGs are due to merge to form a single CCG (Surrey Heartlands CCG). For the purpose of clarity, this policy will be applicable to the above four CCGs until 31/03/20 and for Surrey Heartlands CCG from 01/04/20.

Policy number	CORP 08
Version	1.0
Approved by	Audit Committees
Name of originator/ author	Louise O'Byrne, Governance Lead, East Surrey CCG
Owner (director)	Elaine Newton, Executive Director of Communications and Corporate Affairs
Date of last approval	February 2020
Next approval due	February 2023

Version control sheet

Version	Date	Author	Status	Comments / changes since last version
0.1	September 2019	Audit Committees	Draft	New policy drafted
0.2	14/02/20	Corporate Governance Team	Draft	Extended to include East Surrey CCG. Review and amendments from the following teams: • Security Management Specialist, TIAA • Quality • Health and Safety • Information Governance • Continuing Healthcare • Safeguarding
1.0	21/02/20	Audit Committees	Final	Approved.

Equality Statement

Surrey Heartlands CCG aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. We take into account the Human Rights Act 1998 and promote equal opportunities for all. This document has been assessed to ensure that no employee receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity.

Members of staff, volunteers or members of the public may request assistance with this policy if they have particular needs. If the member of staff has language difficulties and difficulty in understanding this policy, the use of an interpreter will be considered.

We embrace the seven staff pledges in the NHS Constitution. This policy is consistent with these pledges: https://www.gov.uk/government/publications/the-nhs-constitution-for-england/the-nhs-constitution-for-england

See next page for an Equality Analysis of this policy.

Equality Analysis

Equality analysis is a way of considering the effect on different groups protected from discrimination by the Equality Act, such as people of different ages. There are two reasons for this:

- to consider if there are any unintended consequences for some groups
- to consider if the policy will be fully effective for all target groups

Title of Policy: Incident Reporting and Management Policy	**Policy Ref:** CORP08
Assessment conducted by (name, role): Louise O'Byrne, Governance Lead, East Surrey CCG	**Start date for analysis:** 06/02/20 **Finish date:** 06/02/20
Give a brief summary of the policy. Explain its aim. See Section 3	
Who is intended to <u>benefit from</u> this policy? *Explain the aim of the policy as applied to this group.* See Section 3	
1. **Evidence considered:** *What data or other information have you used to evaluate if this policy is likely to have a positive or an adverse impact upon protected groups when implemented?* This policy has been written in line with legal requirements and statutory guidance.	
2. **Consultation:** *Give details of all consultation and engagement activities used to inform the analysis of impact.* N/A	
3. **Analysis of impact:** *In the boxes below, identify any issues in the policy where equality characteristics require consideration for either those abiding by the policy or those the policy is aimed to benefit, based upon your research.* *Are there any likely impacts for this group? Will this group be impacted differently by this policy? Are these impacts negative or positive? What actions will be taken to mitigate identified impacts?*	
a) **Age** Ageism is prejudice or discrimination on the grounds of a person's age. Ageism can affect anybody, regardless of their age	None

b) **Disability** A person has a disability (by law) if they have 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.	None
c) **Gender reassignment** Gender reassignment is a personal, social, and sometimes medical process by which a person's gender appears to others to have changed. Anyone who proposes to, starts or has completed a process to change his, her or their gender is protected from discrimination under the Equality Act. A person does not need to be undergoing medical supervision to be protected.	None
d) **Marriage or civil partnership** This is the relationship between two people who are husband and wife, or a similar relationship between people of the same sex (as defined by Marriage (Same Sex Couples) Act 2013). Civil partners must be treated the same as married couples on a wide range of legal matters.	None
e) **Pregnancy and maternity (adoption is covered within this)** Pregnancy - being pregnant or expecting a baby. Maternity is the period after the birth or adoption and is linked to maternity and adoption leave in the employment context.	None
f) **Race** Race characteristics refers to a group of people defined by their race, colour and nationality (including citizenship) ethnic or national origins.	None
g) **Religion and belief** Religion refers to any religion while belief comprises religious and philosophical beliefs including lack of belief. Generally, a belief should affect your life choices or the way you live for it to be included in the definition.	None
h) **Sex** This is defined as a person's legal sex; in the UK this is recognised as either being a man or a woman. Sex is more commonly referred to as gender identity, which is the internal sense of being male, female, a combination of male and female, or neither male or female.	None
i) **Sexual orientation** Refers to a persons' orientation or attraction towards; the same sex, opposite sex or to both sexes.	None

j) **Carers**[1] A carer is anyone, including children and adults who looks after a family member, partner or friend who needs help because of their illness, frailty, disability, a mental health problem or an addiction and cannot cope without their support. The care they give is unpaid.	None
If any negative or positive impacts were identified are they valid, legal and/or justifiable? Please detail. None	
4. Monitoring: *How will you review/monitor the impact and effectiveness of your actions?* N/A	

[1] Being a carer is not an equality characteristic and is not protected under the Equality Act 2010. However, the CCG is committed to ensuring consideration of their policies and plans on carers.

Contents

1. Introduction

1.1 The aim of this policy and procedure is to outline the arrangements the CCG has in place for reporting, managing and learning from incidents and ensuring that the CCG meets its legal responsibilities in respect of reporting to external agencies. The CCG is committed to the commissioning of high quality care and services and the achievement of a high standard of health, safety and welfare at work for all employees, visitors and other persons engaged in CCG activity.

1.2 The reporting of accidents and incidents is not only a legal requirement but also an essential part of the risk management process. Reporting of all incidents is designed to ensure the following:

- a culture of openness in reporting incidents;
- prompt and accurate information collection;
- support for those affected by an incident;
- identify any trends and prevent or reduce reoccurrences; and
- fulfilment of the CCG's legal and statutory duties under statutory regulations including:
    - RIDDOR 1995,
    - The Health and Safety at Work Regulations 1999,
    - The General Data Protection Regulation, Data Protection Act 2018, and
    - Privacy and Electronic Communications (EC Directive) Regulations 2003.

2. Purpose

2.1 This policy is designed to ensure that all staff have a clear understanding of their responsibilities and respond appropriately and effectively to reporting incidents.

2.2 The purpose of this policy is to:

- define an incident and a serious incident (SI);
- ensure that all staff understand their role and responsibility for incident reporting;
- clearly define the CCG's processes for the reporting, managing and learning from incidents; and
- outline the investigation process and the requirement for escalation

3. Scope

3.1 This policy covers all types of internal CCG incidents and near misses whether clinical or non-clinical, serious or minor and regardless of who was involved. This policy does not apply to commissioned services. Incidents that occur within NHS provider organisations should be reported and investigated internally in accordance with that provider organisation's policy. This is in line

3.2 with Health and Safety legislation, the National Patient Safety Agency (NPSA) guidance and requirements of relevant regulatory bodies e.g. the Medicines and Healthcare products Regulatory Agency (MHRA). However, independent contractors and managers of contracted services must notify the CCG of:

- all serious incidents in line with the NHSE Serious Incident Framework;
- all significant trends in incidents;
- incidents with significant learning opportunities for other independent contractors; and
- any serious incident that may impact on the obligations outlined within the contract.

3.3 Further information in regard to process followed by the CCG to gain the necessary assurances for the management of SIs can be found in the Surrey Heartlands CCG Serious Incident Policy (CORP 03).

3.4 This policy applies to all incidents including near miss incidents and is applicable to all CCG staff, regardless of whether they are directly employed or hold a corporate or clinical role and includes:

- individuals on the CCG Governing Body, committees and sub-committees;
- employees of the CCG including staff on secondment;
- third parties acting on behalf of the CCG;
- agency, locum and other temporary staff engaged by the CCG; and
- visitors to the CCG and members of the public

4. Fair and Open Culture

4.1 The CCG recognises that an incident, however serious, is rarely caused wilfully and is not necessarily evidence of carelessness, neglect or a failure to carry out a duty of care. Errors are often caused by a number of factors including human error, individual behaviour and lack of knowledge or skills.

4.2 Learning from incidents can only take place when incidents are reported and investigated in a positive, open and structured way.

4.3 The CCG supports and promotes an open, fair and positive learning culture to support staff and help improve the safety and quality of the CCG, and reflects a duty of candour as described in the Francis Report (2013).

4.4 A non-punitive approach to the incidents reported will be taken unless there is evidence of gross professional or gross personal misconduct; repeated breaches of acceptable behaviours or protocol; or where a staff member has become subject of a police investigation. For these incidents the appropriate HR policies will be adhered to. This is in accordance with the CCG's Raising Matters of Concern (Whistleblowing) Policy which provides an anonymous system enabling staff to raise concerns, without fear of suffering any adverse consequences as a result.

5. Definitions

5.1 Incident

5.1.1 An incident is any accident, event or circumstance that could or did lead to harm, loss or damage to people, property, reputation, or other occurrence that could impact on the organisation's ability to achieve its objectives.

5.1.2 Examples of an incident may include one or more of the following:

- personal accidents resulting in harm or injury, however minor;
- equipment failure, loss or damage;
- all health and safety related incidents;
- fire or fire alarm activations;
- physical and/or verbal aggression, assault or abuse, sexual or racial harassment, instances of bullying, intimidation or threatening behaviour;
- clinical incidents;
- work or environmental related incidents;
- Security issues including vandalism, property loss or damage, theft; and
- Incidents involving vehicles.

5.1.3 Information Governance (IG) incidents are defined in a more specific way, detailed in Section 9.1 of this policy.

5.2 Near miss

5.2.1 A near miss is any near incident that did not actually lead to harm, loss or damage but had potential to do so. Reporting near misses is vital, as they may identify the need for changes in procedures, processes and systems which could prevent further similar occurrences from causing actual harm, loss or damage.

5.2.2 Examples of a near miss may include one or more of the following:

- A slip or trip with no injury resulting

- Defective or damaged equipment in use with no injury resulting
- Substance causing a potential slipping hazard

5.3 Serious Incident (SI)

5.3.1 The NHS Serious Incident Framework 2015 describes a serious incident as an incident that occurred during NHS funded healthcare which resulted in one or more of the following:

- an unexpected or avoidable death or severe harm to one or more patients, staff or member of the public;
- a "Never Event" (as outlined in the NHS Never Events Policy and Framework);
- a scenario that prevents, or threatens to prevent, an organisation's ability to deliver healthcare services, including data loss, property damage or incidents in population programmes (e.g. screening and immunisation) where harm may potentially extend to a large population;
- allegations, or incidents of physical/ sexual abuse or assault; and
- loss of confidence in the service, adverse media coverage or public concern about healthcare or an organisation.

5.3.2 Most serious incidents are provider reportable and are quality assured by the CCG, details of which can be found in the Surrey Heartlands CCG's Serious Incident Policy However, there may be circumstances where the CCG is required to report an SI. These must be reported and investigated in accordance with the Serious Incidents policy.

6. Duties and responsibilities

6.1 Accountable Officer

6.1.1 The Accountable Officer has overall responsibility for safety and is accountable for ensuring the CCG has the necessary systems in place to enable the effective reporting, management and investigation of incidents.

6.2 Executive Directors

6.2.1 Executive Directors have a responsibility to support the Accountable Officer in the implementation of this policy and in monitoring its effectiveness. Executive Directors will actively promote and support the reporting of incidents as per the CCG's fair and open culture, whilst ensuring that all direct reports are aware of and undertake their responsibilities in relation to incident reporting.

6.3 Managers

6.3.1 Line managers are responsible for ensuring that staff are aware of this policy and that they report incidents when they occur. Line managers are required to support

staff when an incident occurs, and to have an active role in assessing the situation, ensuring that the incident is reported and investigated appropriately.

6.4 Staff

6.4.1 All staff have a responsibility to report all incidents in accordance with this policy and have a duty to patients, their employer and colleagues to co- operate fully with any investigation, in order to ensure the most appropriate outcome.

6.5 Risk Team

6.5.1 The Risk Team is responsible for ensuring that the organisation has robust systems and processes in place to ensure effective incident management. The team will liaise with other staff members to provide appropriate advice when required. The team will receive and review information about reported incidents to ensure that issues have been addressed and recommendations for improvements have been implemented. The team will provide organisational analysis to ensure learning is shared across the CCG.

6.6 Specialist Review

6.6.1 The Surrey Heartlands CCG Incidents Database (Datix) is set up to divert incidents directly to nominated colleagues within the following teams as soon as they are reported under one of these categories for specific actions:

- Information Governance;
- Health and Safety; and
- Continuing Healthcare (CHC)

6.6.2 For other incidents, the Risk Team will contact relevant managers to request specialist input into the reporting, investigation, analysis and review of incidents, as appropriate.

6.7 IG incidents – responsibilities

6.7.1 The Senior Information Risk Owner (SIRO), Caldicott Guardian & IG Team members have specific roles with regard to IG incidents, which are set out in Annex 4 of the Surrey Heartlands' *Data Protection & Confidentiality Policy*.

7. Process for Reporting an Incident

7.1.1 When an incident occurs, the immediate priority is to take steps to ensure the safety of the people involved. Actions will vary depending on the type of incident, but could include administering first aid, contacting the emergency services, removing faulty equipment or changing current practice to prevent reoccurrence. Staff will need to consider whether the incident meets the serious incident criteria by referring to the Serious Incident Policy, discussing with their line manager and also seeking advice from the Integrated Care Partnership or Integrated Care System Quality Lead as appropriate.

7.1.2 Any incident which raises safeguarding concerns will be automatically directed to the CCG safeguarding team for review. All reports will be submitted via the Datix system with the on-line reporting form allowing for a box to be checked to indicate safeguarding concerns.

7.1.3 The process for reporting an IG incident is detailed in section 9.1.

7.1.4 It is the responsibility of all staff to inform the appropriate manager and report an incident within two working days of identifying its occurrence (or 24 hours if serious). All incidents should be reported via the CCG's online incident report form. This can be accessed via Datix. The link is available on the CCGs intranet or via the desktop.

7.1.5 It should be noted that internal reporting does not affect the need to call emergency services if they are needed, or to report to the police if necessary.

7.1.6 The form should be completed by the person involved in the incident, or by a witness if that person is unable to complete the form. All required fields on the form must be completed using the facts known rather than opinions. This information may be required in support or defence of legal action. In the event of a fatality, major incident, case of disease or other incidents which may have major implications, the Accountable Officer must be informed as soon as possible (via the on call system if necessary).

7.1.7 In the description of the incident, as much detail as possible should be provided. If inappropriate language is used in assault cases, this should be reflected in the description, in order to reflect severity of the situation.

7.1.8 Once an incident has been logged an appropriate individual will be allocated to lead the investigation, by the Information Governance, Health and Safety, CHC or Risk Team as appropriate. The investigator will need to confirm whether external organisations need to be informed (see appendix A for further details).

7.1.9 Once an investigation has concluded the results, actions and lessons learned must be recorded on Datix. It is the responsibility of the investigating manager to ensure feedback has been provided to the person reporting the incident.

7.1.10 For all serious incident investigations a comprehensive investigation report outlining the root cause, contributory factors, lessons learned and a detailed action plan to address all recommendations will be produced – please refer to the Surrey Heartlands CCG Serious Incident Policy for details.

7.1.11 An overview of the incident reporting process can be found in appendix B.

8. Investigating an Incident

8.1 All incidents require some level of investigation in order to identify the underlying causes of why the incident occurred. The depth and breadth of an investigation should be proportionate to the level of risk posed by the recurrence of similar incidents.

8.2 Investigations should:

- ensure timely and appropriate follow-up;
- be completed within 30 working days, or 60 working days for serious incidents;
- establish the facts;
- identify the root cause and any contributing factors;
- identify all actions to be taken as a consequence, to prevent, as far as practicable, similar incidents occurring in future; and
- meet national, regional and legal reporting requirements.

8.3 To support staff in the investigation of incidents, appropriate specialist reviewers may be asked by the Risk Team to support the process.

8.4 The model for investigations at all levels is based on the principles of the root cause analysis (RCA) technique. The underpinning notion behind RCA is that systems and processes should be reviewed to identify the potential causes of failure, and that corrective actions should be subsequently taken to prevent reoccurrence.

8.5 Appendix C provides further guidance on how to conduct an incident investigation. There are many different methodologies which can be utilised to conduct a root cause analysis investigation, and the most appropriate tool will depend on the investigation. The Risk Team will be able to advise and provide supporting material to assist lead investigators.

9. Types of Incidents

9.1 Information Governance Incidents

9.1.1 An IG incident is a personal data breach meaning a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal or other confidential data transmitted, stored or otherwise processed.

9.1.2 An IG incident can include any breach of the CCG's IG related policies, applicable legislation, or NHS requirements. IG incidents can therefore include a diverse range of situations including:

- lost staff identity badge or desk pedestal keys;
- mislaid documents including confidential information;
- access to patient identifiable data by someone who does not have a need to know;
- lost or stolen CCG issued lap-top, mobile phone, or USB drives;

- hacking of electronic data or attack by a computer virus or other malicious software;
- clicking on a link or attachment within a phishing email; and
- ransomware attack.

9.1.3 All IG breaches will be managed in accordance with NHS Digital's Guide to the Notification of Data Security and Protection Incidents and Annex 4 of the CCG's Data Protection and Confidentiality Policy.

9.1.4 All IG incidents must be reported immediately via Datix in line with this policy and Annex 4 in the CCG's Data Protection and Confidentiality Policy. This is due to the requirement to externally report applicable breaches within 72 hours. If for any reason the incident cannot be reported on Datix, the CCG's IG Team must immediately be notified via email to: gwccg.informationgovernance@nhs.net

9.1.5 Upon reporting an IG incident on Datix, the incident will automatically be referred to the CCG's IG Team. The IG Team will review the incident to confirm whether it needs to be reported to NHS Digital and the Information Commissioner's Office via NHS Digital's Data Security and Protection Toolkit Incident Reporting Tool, in liaison with the Senior Information Risk officer (SIRO) and Caldicott Guardian; and/or if the incident should be escalated internally.

9.2 Health and Safety, Fire, Security and Environmental Incidents

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

9.2.2 All health and safety, fire, security or environmental incidents should be reported via Datix in line with this policy. Upon reporting, these incidents will automatically be forwarded to the CCG's Senior Business Support and Facilities Manager and/or nominated deputy/ies, who will review the incident to confirm whether it needs to be externally reported and nominate an investigator.

9.2.3 The organisation is statutorily obliged to report in the Report of Injuries, Diseases and Dangerous Occurrences Regulations 1995, (RIDDOR) incidents to the Health and Safety Executive (HSE). Incidents must be reported under RIDDOR when someone has been absent from work for more than seven days due to an incident. The investigating officer will report the incident to the HSE. Advice on whether an incident is RIDDOR reportable can be obtained from the Senior Business Support and Facilities Manager.

9.3 Continuing Healthcare Incidents

9.3.1 Continuing Healthcare (CHC) staff should report incidents using the same process as outlined above. When an incident is reported as a CHC incident, it is automatically forwarded to a nominated individual(s) within the CHC team, as well as the Safeguarding team if appropriate. As with all other types of incident, if the incident meets SI criteria the SI policy must be followed.

9.3.2 With incidents relating to Information Governance (IG) that originate from work carried out by/for the CHC team, these should be recorded as an IG incident and not a CHC incident. Therefore, the IG team would receive the incident in the first instance, and open an investigation

9.4 Safeguarding

[Under review.].

9.4.1 The DATIX incident report form contains a field to check if there are any suspected safeguarding issues. In this way, the system ensures that all incidents are reviewed for any safeguarding issues. If there are safeguarding concerns then an automatic request for a safeguarding referral is generated. All incidents logged with safeguarding issues create an automatic alert to the CCG Safeguarding team for review and input if required.

9.5 Fraud, Bribery and Corruption Incidents

9.5.1 Incidents and suspected incidents of Fraud, Bribery or Corruption are out of the scope of this policy. Please refer to the CCG's Anti-Fraud Bribery and Corruption Policy for guidance on the reporting of such incidents. **Please do not report incidents of Fraud, Bribery or Corruption via Datix**, as this could seriously undermine the investigations of the Local Counter Fraud team.

9.6 Serious Incidents (SIs)

9.6.1 This section highlights some key points from the CCG's Serious Incidents Policy. Please refer to the full policy if you need to report a Serious Incident.

9.6.2 All incidents involving the CCG must be reported as an incident according to this policy, and will be reviewed to ascertain whether the incident falls into the category of a serious incident. Within a CCG, incidents meeting this criteria are likely to be non-clinical, or staff related incidents. However, the CCG does have a CHC Team who may report a number of clinical incidents relating to the safeguarding of vulnerable adults, which may fit the SI criteria.

9.6.3 If a member of staff reports an incident which they deem to meet the serious incident criteria then this should be flagged on the reporting form in Datix. The investigating officer will then escalate this to the appropriate Head of Service (IG; EPRR, Facilities Management and Business Support; CHC; Governance), who will decide in association with the Head of Quality-Safety and the appropriate Director whether the incident meets the criteria for a Serious Incident (SI) in accordance with the NHS framework.

9.6.4 On agreement that the incident is an SI, an email is sent to the Surrey Heartlands generic SI box and a SI notification form is completed as per the process detailed in the Surrey Heartlands CCG Serious Incident Policy, via the national Strategic Executive Information System (STEIS). In line with nationally agreed timeframes, such incidents must be reported within 2 working days of the incident being identified.

9.6.5 The relevant Director will appoint an appropriate lead investigator with support from the relevant team and/or the Risk Team.

9.6.6 The investigation process for SIs will follow the same process as the incident investigation process outlined within this policy.

9.6.7 All SI final investigation reports will be submitted to the generic SI email inbox.

10. Sharing and Embedding Learning

10.1 Learning from incidents is critical to the delivery of safe and effective services within the CCG. Each incident and subsequent findings ensuing from the investigation are a learning opportunity. These lessons will be shared across the organisation using the following methods:

- information will be published in the CCG staff bulletin and on notice boards where appropriate;
- immediate lessons learned will be shared through the Team Brief;
- reports will be presented to the appropriate CCG committee; and
- the CCG will take the opportunity to share lessons learnt across the health and social care system through networks and consortiums, and in cooperation with partner organisations where appropriate.

10.2 In terms of reporting, Datix is capable of producing a range of reports based on all of the information fields and variables on the Datix incident reporting/management system at regular intervals. These reports can be tailored to the specific needs of the organisation via directorates, teams or committees. They can be used to feed back information on trends, lessons learned and actions taken.

10.3 An overview of incidents reported across the organisation will be monitored for trends, themes and lessons learned through reporting to appropriate committees

10.4 The CCG Head of Governance and Risk will also receive a non-clinical incident report at the beginning of each month.

11. Support for staff

11.1 The CCG is committed to learning from incidents and improving safety in a systematic and non-blaming manner, and recognises that staff work within systems and processes which may themselves contribute to incidents occurring. It is also recognised that during the course of an investigation, issues concerning individuals' standards may be identified. If this occurs, this will be addressed separately to internal investigation processes, via HR processes.

11.2 The CCG recognises that investigations may be potentially stressful for staff. Line managers will be automatically notified, and should ensure that individual support

needs are discussed, and that information about how to access appropriate support services is provided.

12. Duty of Candour

12.1 The CCG will also ensure that Duty of Candour is applied when appropriate. Duty of Candour is the requirement for organisations to ensure that affected patients/families are informed of errors resulting in moderate/severe harm or death, and provided with appropriate support. This includes providing an apology, as appropriate, and ensuring that the investigation findings and agreed actions are shared

13. Monitoring Compliance and Effectiveness

13.1 The incident reporting process will be reviewed periodically by the Risk Team to ensure the following:

- incident forms are completed correctly;
- regular data quality checks of the CCG's reporting system (DATIX) to identify coding errors, under-reporting and inappropriate reporting;
- action plans are produced and objectives are specific, measurable, achievable, realistic and timely (SMART) and implemented with outcomes monitored;
- persons throughout the incident reporting process understand their roles and responsibilities and have the capabilities to contribute effectively to the incident reporting process; and
- relevant timescales, both internal and external, are adhered to.

13.2 Incident reporting is reviewed through the CCG committee structure as follows:

Committee	Responsibilities
Governing Body	• Overall accountability for safety. • Accountable for the risk management strategy, systems and processes including incident reporting.
Audit Committee	• Accountable for ensuring that the governing body is assured of the effectiveness of the systems and processes for supporting and improving safety. • Approves the policy and procedure for the management of incidents
Health & Safety Committee	• Receives reports regarding health and safety incidents, reviews lessons learnt and identifies the necessary actions required. • Ensures action plans are fully implemented. • Agree on bulletin agendas to support sharing wider learning.

Committee	Responsibilities
IG Sub-Committee	• Recommend or undertake remedial action following reported breaches of IG. • Receives reports regarding information governance incidents, reviews lessons learnt and identifies any further actions required. • Ensures action plans are fully implemented. • Agree on bulletin agendas to support sharing wider learning
SI panels	• Receive and review serious incident investigation reports to ensure they meet the requirements of a robust root cause analysis investigation as set out in national guidance.

For further information regarding the role of these committees please see individual terms of reference

14. Education and training requirements

14.1 **All New Starters**: An introduction to incident reporting will be included in the CCG's induction programme. An IG specific induction for all new starters will include IG incident reporting.

14.2 **Existing Staff:** As incident management policies and processes are developed, staff will be updated and where necessary undertake appropriate further training to meet their needs.

14.3 All staff are required to undertake statutory and mandatory training which includes health and safety, information governance and safeguarding training. Further information can be found in the CCG's Statutory and Mandatory Training Policy.

15. Monitoring and Review

15.1 This policy will be subject to review by the Audit Committee a minimum of every three years. More frequent reviews will take place if required.

16. Associated documentation

16.1 This policy is linked to the following CCG policies and strategies:

- Surrey Heartlands CCG Serious Incident Policy;
- Risk Management Strategy;
- Health and Safety Policies;
- Compliments, Concerns, Comments & Complaints Policy and Procedures
- Whistleblowing Policy;
- Records Management Policy;

- Safeguarding Adults and Children Policy in conjunction with Surrey Safeguarding Adults procedures; and Surrey Safeguarding Children Manual procedures
- Statutory and Mandatory Training Policy;
- Anti-Fraud, Corruption and Bribery Policy; and
- Data Protection and Confidentiality Policy.

16.2 This policy and procedure takes into account:

- the Health & Safety at Work Act etc. 1974;
- the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) (2013);
- guidance from the NHS Counter Fraud Security Management Service;
- Management of Health & Safety at Work Regulations (1999);
- Care Quality Commission Essential Standards of Quality and Safety (2009);
- National Patient Safety Agency Guidance;
- NHS England Serious Incident Framework (2015)
- the General Data Protection Regulation;
- the Data Protection Act (2018); and
- NHS Digital's Guide to the Notification of Data Security and Protection Incidents.

17. Appendix A: External Reporting

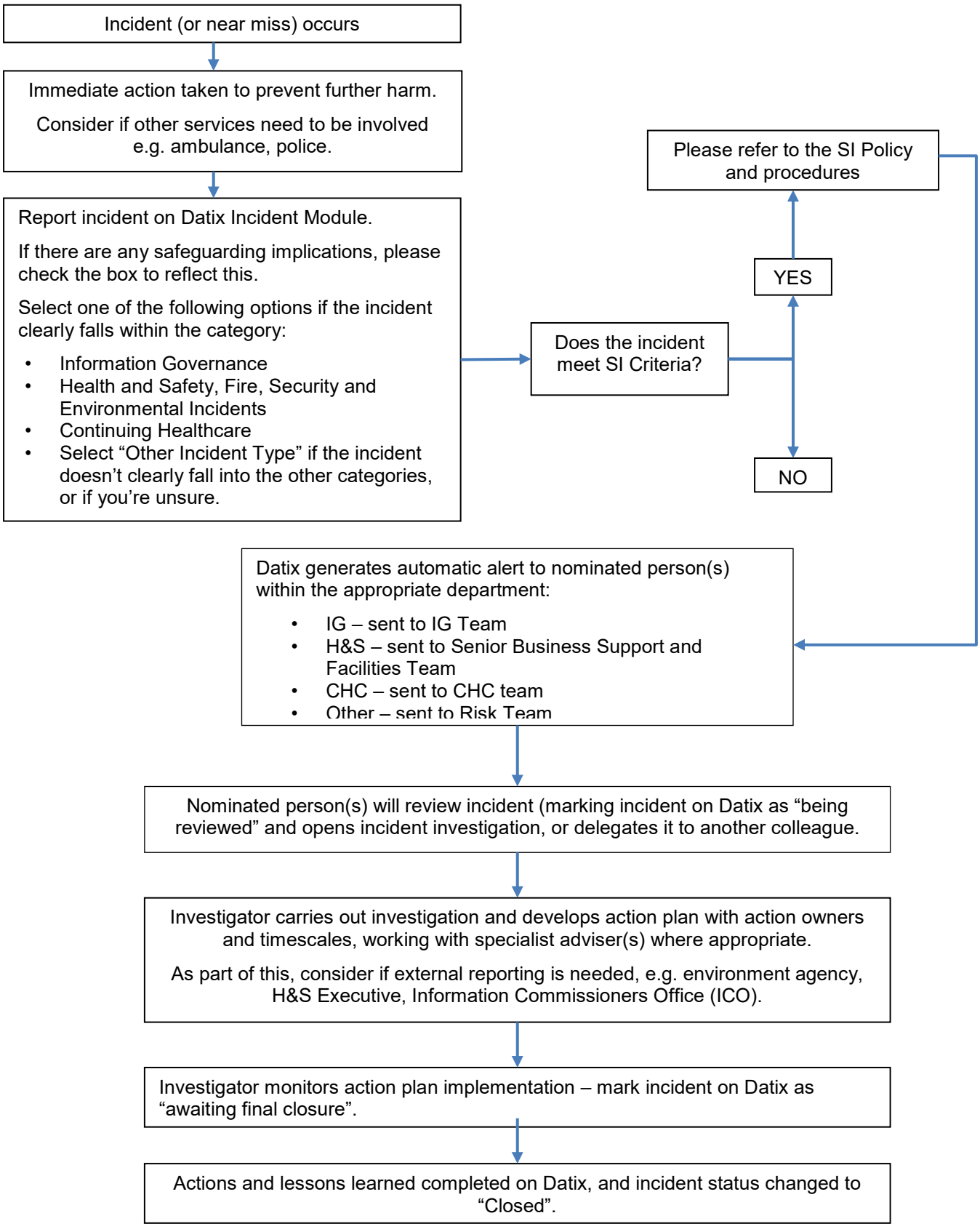
17.1 In addition to internal reporting, certain categories of incident require reporting to external agencies. The following table outlines the incident types and the receiving agency.

Incident Type	Reportable to
Patient Safety Incidents.	National Reporting and Learning Service (NRLS). NB this will happen automatically through Datix via monthly uploading of data.
RIDDOR – Injuries to staff sustained in the course of work including: • Any incident which results in staff absence for more than seven consecutive days as the result of their injury. This seven-day period does not include the day of the accident, but does include weekends and rest days. The report must be made within 15 days of the incident; • major injuries e.g. fracture, amputation, loss of sight, electric shock; and • diseases contracted in the course of work, e.g. occupational dermatitis, asthma, hepatitis, tuberculosis, tetanus etc. http://www.hse.gov.uk/riddor/	Health & Safety Executive
Physical Assault on Staff.	NHS Security Management Service. Police.
Externally reportable Information Governance Incidents.	NHS Digital's Data Security and Protection Toolkit Incident Reporting Tool notifies both NHS Digital and the Information Commissioner's Office.
Serious Incidents.	Strategic Executive Information System NHSE.

17.2 The investigating officer is responsible for reporting incidents to relevant external organisations, where applicable. This will be supported by expert advisors when required. The above list is not definitive and will depend on the incident that has occurred.

18. Appendix B: Incident Reporting Process Overview Flow Chart

18.1 This flow chart applies to near misses as well as incidents



19. Appendix C: Guidance for Carrying out an Investigation

19.1 Arrangements for appointing an investigating officer will be made locally by each of the four responsible teams (Information Governance; Health and Safety; CHC; Risk)

19.2 An investigation should commence immediately, where safe and legal to do so. The objective of the investigation is not to apportion blame or liability but to identify what happened and **WHY** the incident occurred.

19.3 An investigation is a systematic process with the purpose of uncovering and clarifying the central issues, thereby making it easier to establish facts, context, contributory factors and root causes, and to enable the identification of solutions to minimise recurrence. Advice relating to incident investigation can be sought from the Risk Team.

19.4 Timescale for conducting investigations

19.4.1 A final report including an action plan must be entered onto Datix within **30 working days** of the incident being reported.

19.4.2 A good investigation is both prompt and thorough. Failure to conduct an investigation as soon as practicable after the event can result in difficulties in obtaining relevant information and evidence, as conditions change and memories of the incident may fade. It is extremely important therefore that the investigation is undertaken without any undue delay. The lead investigating officer will be responsible for agreeing any revised timescale with the parties concerned.

19.4.3 The investigating officer will decide on the requirements for the investigation team dependant on the seriousness of the incident. This may include a CCG Director and specialist advisors where appropriate.

19.5 Evidence

19.5.1 The sources of information and methods which investigators can use typically fall into the following three categories:

- direct observation of where the event occurred, which is important to avoid losing important evidence about the scene, configuration, relationships between parties, etc;
- collecting data/documentation, which helps establish what should have happened as well as providing evidence of prior risk assessment, inspections, tests, witness statements etc; and
- interviews which, when conducted sensitively, provide both direct testimony as well as an opportunity to check back on any issues arising from examination of the physical and documentary evidence.

19.5.2 Although direct observation, collecting data and interviews are distinct and important elements of a thorough investigation, they complement each other. They

provide an opportunity to 'read across' from one part of the process to another to check reliability and accuracy as well as resolve differences and gaps in evidence.

19.6 Root Cause Analysis (RCA)

19.6.1 Some incidents may require a root cause analysis to be undertaken as part of the investigation process, in order to identify the contributing factors and underlying causes of why the incident occurred.

19.6.2 The Root Cause Analysis Process is outlined below:

1: Information Gathering: Gather all appropriate information required e.g. from staff involved; site of incident; related policies & procedures; patient records.

2: Information Mapping: Complete the time line/ chronology in order to get the full picture of the incident as it unfolded.

3: Identify problems and highlight good practice: Within the chronology identify where things began to go wrong and why. Highlight good practice.

4: Identify the Contributory Factors: Having identified the problems, undertake a fishbone of each problem to identify the contributory factors.

5: Agree the Root Cause/s: Identify which of the above factors most contributed to the incident and which had they been prevented, the incident would not have occurred

6: Generate Solutions: By rectifying the system/ process at this point should prevent the incident from reoccurring.

7: Recommending and Reporting: Ensure the recommendations made will prevent a similar incident in the future.

19.6.3 Root Cause Analysis Tools: A complete set of investigative tools are available via http://www.nrls.npsa.nhs.uk?resources/collections/root-cause-analysis/

19.7 Further advice can be sought from the Risk Team.

20. Appendix D – Procedural Document Checklist for Approval (under review)

Title of document being reviewed:		Yes/No/ Unsure	Comments/ Details
A	**Is there a sponsoring director?**		
1.	**Title**		
	Is the title clear and unambiguous?		
	Is it clear whether the document is a guideline, policy, protocol or standard?		
2.	**Rationale**		
	Are reasons for development of the document stated?		
3.	**Development Process**		
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?		
	Is there evidence of consultation with stakeholders and users?		
4.	**Content**		
	Is the objective of the document clear?		
	Is the target group clear and unambiguous?		
	Are the intended outcomes described?		
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?		
	Are key references cited?		
6.	**Approval**		
	Does the document identify which committee/group will approve it?		
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how the document will be disseminated and implemented amongst the target group? Please provide details.		
8.	**Process for Monitoring Compliance**		

Title of document being reviewed:		Yes/No/ Unsure	Comments/ Details
	Have specific, measurable, achievable, realistic and time-specific standards been detailed to monitor compliance with the document? Complete Compliance & Audit Table.		
9.	**Review Date**		
	Is the review date identified?		
10.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for implementing and reviewing the documentation i.e. who is the document owner?		

Approval			
Executive Director Name		Signed off on (date)	
Committee Chair Name		Signed off on (date)	
On behalf of the		Approved on (meeting date)	

21. Appendix E – Compliance and Audit Table (under review)

Criteria	Measurable	Frequency	Reporting to	Action Plan/ Monitoring