

INCIDENT POLICY

POLICY REFERENCE NUMBER	RM012
DATE RATIFIED <i>(this version)</i>	June 2015
NEXT REVIEW DATE	December 2018
APPROVED BY <i>(state group)</i>	Quality and Safety Sub-committee
ACCOUNTABLE DIRECTOR	Executive Director of Nursing and Quality
POLICY AUTHOR	Associate Director of Patient Safety & Quality Governance

Policy Statement/Key Objective:

This policy provides a consistent and thorough approach to the reporting, management and investigation of all incidents. It aims to facilitate openness, trust, continuous learning and service improvement.

Executive Summary

Title of Policy:	Incident Policy
Subject:	This policy provides a consistent and thorough approach to the reporting, management and investigation of all incidents. It aims to facilitate openness, trust, continuous learning and service improvement.
Applicable to: <i>(state Network, Services and staff groups)</i>	All staff
Key Policy Issues:	To ensure a consistent and thorough approach to the reporting, management and investigation of all incidents
Original Issue Date:	November 2010
Issue Date <i>(this Version - including any minor amendments)</i>	June 2015
Dates Policy Reviewed: <i>(include all previous dates of review)</i>	April 2011, December 2012, August 2014, October 2014
Next Review Date:	October 2017
Policy written by: <i>(state title only)</i>	Associate Director of Patient Safety and Quality Governance
Policy Lead: <i>(state title only)</i>	Associate Director of Patient Safety and Quality Governance
In Consultation with:	Serious Incident Advisory Group, Risk Team, commissioners and Networks
Monitoring Arrangements:	See section 7
Approved by: <i>(state group)</i>	Quality and Safety Sub-committee
Authorised by: <i>(state senior accountable person e.g. Network or Clinical Director)</i>	Executive Director of Nursing and Quality
Related Procedural Documents:	Quality Strategy, Risk Management Policy, Being Open Policy, Health and Safety Policy, Safety Alerts Policy

Table of Contents

1.0	Introduction	4
2.0	Scope.....	4
3.0	Definitions.....	5
4.0	Duties	7
5.0	The Policy	11
5.1	Incident reporting	11
5.2	External incident reporting	12
5.3	Incident management	13
5.4	Incident investigation	13
5.5	Regulatory investigations.....	16
5.6	Coroners inquests.....	17
5.7	Safeguarding incidents	17
5.8	Infection control incidents	17
5.9	Deaths in custody	18
5.10	Police involvement.....	18
5.11	Trade union involvement.....	18
5.12	Learning from incidents.....	19
5.13	Being Open (Duty of Candour)	20
5.14	Support for staff	20
6.0	Training	20
7.0	Monitoring.....	21
7.0	References	21
	Appendix 1 – Incident Reporting and Management Process	23
	Appendix 2 – Serious Incident Investigation Process	24
	Appendix 3 – Safeguarding Incident Investigation Process	25
	Appendix 5 – Incident Level Guidance.....	26
	Appendix 6 – Externally Reported Incidents (STEIS/RIDDOR etc.).....	28
	Appendix 7 – Never Events	35
	Appendix 8 – Incident Decision Tree.....	37

1.0 Introduction

- 1.1 Lancashire Care NHS Foundation Trust (hereafter referred to as “LCFT” or “the Trust”) is committed to enhancing the safety of its patients, staff, carers and the public by ensuring that it has valid systems to report and learn from adverse events. This policy sets out the systems, processes and requirements for incident reporting, management, investigation and learning.
- 1.2 This policy is based on the following principles:
- A culture of learning and openness is required to improve safety and effectiveness and all managers must support the development of this culture;
 - All incidents should be reported and managed efficiently and effectively;
 - The needs of those affected should be the primary concern of those involved in the response to and the investigation of serious incidents. Patients and their families/carers and victims’ families must be involved and supported throughout the investigation process in accordance with the Being Open Policy and statutory duty of candour;
 - Information from incidents should be made available to all levels of the Trust to inform improvements to service and care delivery;
 - The Trust will cooperate with other providers, commissioners and regulators to support the investigation of incidents and subsequent learning;
 - Investigations are conducted for the purposes of learning to prevent recurrence. They are not conducted to hold any individual or organisation to account as other processes exist for that purpose including: criminal or civil proceedings, disciplinary procedures, employment law and systems of service and professional regulation, such as the Care Quality Commission and the Nursing and Midwifery Council, the Health and Care Professions Council, and the General Medical Council.

2.0 Scope

- 2.1 This policy applies to all incidents and near misses, whether clinical or non-clinical, in order to provide a consistent approach to incident reporting and management.
- 2.2 It applies to all employees of the Trust (including temporary, bank and agency staff) and any other persons whose activities may directly or indirectly affect patients, visitors, staff and the organisation.
- 2.3 This policy aims to facilitate learning by promoting a fair, open, and just culture that abandons blame as a tool and promotes the belief that incidents cannot simply be linked to the actions of the individual staff involved but rather the

system in which the individuals were working. Looking at what was wrong in the system helps organisations to learn lessons that can prevent the incident recurring.

2.4 Whilst adopting a systems improvement approach, this policy recognises that there will be occasions when safety is compromised because of serious misconduct by individual members of staff. The Incident Decision Tree (Appendix 8) should be used to determine the appropriate response. The member of staff should be removed from the incident investigation and a disciplinary investigation commenced when:

- There is a breach of criminal law;
- There is evidence or suspicion that the actions leading to harm (including acts of omission) were reckless, grossly negligent or wilfully neglectful;
- There is evidence or suspicion that harm/adverse consequences were intended;
- Serious professional misconduct has been identified;
- There are repeated unsafe occurrences in relation to the same individual;
- There is evidence that attempts were made to conceal the incident or tamper with any evidence;
- There is evidence that false information was provided to the investigation.

2.5 The Trust will not tolerate any attempts to impede or punish employees for using the Trust's incident reporting policy and systems. Should an employee not feel safe in reporting an incident they should use the Trust's Raising Concerns Policy which allows for anonymous reporting and provides a Raising Concerns Guardian and a network of champions to support employees.

3.0 Definitions

3.1 Incident

An incident is an event or circumstance that resulted in or could have resulted in unnecessary damage, loss or harm such as physical or mental injury to patients, staff, visitors or members of the public and damage to the organisation, its resources, reputation and operations.

3.2 Near Miss Incident

Near miss situations are where an incident was prevented by some form of intervention (either deliberate or inadvertent) and so resulted in no harm but without the intervention may have resulted in harm.

3.3 Serious Incident (SI)

In broad terms, serious incidents are events in health care where the potential for learning is so great, or the consequences to patients, families and carers,

staff or organisations are so significant, that they warrant using additional resources to mount a comprehensive response. Serious incidents can extend beyond incidents which affect patients directly and include incidents which may indirectly impact patient safety or an organisation's ability to deliver ongoing healthcare services. Serious Incidents in the NHS include:

- Acts and/or omissions occurring as part of NHS-funded healthcare (including in the community) that result in:
 - Unexpected or avoidable death of one or more people. This includes suicide/self-inflicted death and homicide by a person in receipt of mental health care within the recent past;
 - Unexpected or avoidable injury to one or more people that has resulted in serious harm;
 - Unexpected or avoidable injury to one or more people that requires further treatment by a healthcare professional in order to prevent the death of the service user or serious harm;
 - Actual or alleged abuse; sexual abuse, physical or psychological ill-treatment, or acts of omission which constitute neglect, exploitation, financial or material abuse, discriminative and organisational abuse, self-neglect, domestic abuse, human trafficking and modern day slavery;
- A Never Event;
- An incident (or series of incidents) that prevents, or threatens to prevent, an organisation's ability to continue to deliver an acceptable quality of healthcare services;
- Major loss of confidence in the service, including prolonged adverse media coverage or public concern about the quality of healthcare or an organisation.

A more detailed list with supporting definitions is available at Appendix 6.

3.4 Never Events

Never Events are a particular type of serious incident that are wholly preventable and where guidance or safety recommendations that provide strong systemic protective barriers are available at a national level, and should have been implemented by all healthcare providers.

A list of applicable never events to the Trust is detailed at Appendix 7.

3.5 RIDDOR Incidents

The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR) requires employers to report deaths, certain types of injury, some occupational diseases and dangerous occurrences that 'arise out of or in connection with work'. Generally, this covers incidents where the work activities, equipment or environment (including how work is carried out, organised or supervised) contributed in some way to the circumstances of the incident.

A list of applicable RIDDOR incidents to the Trust is detailed at Appendix 6.

3.6 Externally reportable incidents

A comprehensive list of incidents that the Trust is required to report to external organisations is included at Appendix 6. External reporting of incidents will be undertaken by the lead department as set out in this policy.

3.7 Datix

Datix is a web based risk management system that can be accessed by any Trust computer via the Trust intranet home page. A module of the Datix system is dedicated to the reporting and management of incidents.

4.0 Duties

4.1 The **Executive Director of Nursing and Quality** is responsible for:

- Acting on behalf of the **Chief Executive** to ensure there are robust policies, systems and processes for the reporting, investigation, management and learning from incidents;
- Reviewing new serious incidents with the Medical Director and determining a further level of investigation, taking action where necessary to address immediate concerns;
- Commissioning and leading the development of thematic analysis and quality surveillance in relation to incidents and learning from incidents;
- Taking action where appropriate to ensure the safety of people and services.

The Director of Nursing and Quality will be supported in these duties by the Associate Director of Patient Safety and Quality Governance who will act on delegated authority.

4.2 The **Medical Director** is responsible for:

- Reviewing new serious incidents with the Director of Nursing and Quality and determining a further level of investigation, taking action where necessary to address immediate concerns;
- Commissioning and leading the development of thematic analysis and quality surveillance in relation to incidents and learning from incidents;
- Taking action where appropriate to ensure the safety of people and services;
- Undertaking the role of Caldicott Guardian by ensuring systems are in place for information governance incidents to be properly reported and managed in accordance with this policy.

The Chief Pharmacist (in their role as Controlled Drugs Accountable Officer) will act on behalf of the Medical Director in relation to medications safety and in ensuring national requirements and guidance are implemented.

4.3 The **Associate Director of Patient Safety and Quality Governance** is responsible for:

- Developing and implementing robust policies, systems and processes for the reporting, investigation, management and learning from incidents (including ensuring compliance with legislation and NHS standards in relation to incidents such as ensuring appropriate and timely external reporting);
- Developing and implementing systems to provide assurance of the Trust's compliance with policies, systems and processes for the reporting, investigation, management and learning from incidents, addressing or escalating matters of non-compliance (this includes providing assurance to the Board, Executive Management Team, Quality Committee and Quality and Safety Sub-committee);
- Determining whether an incident meets the criteria for external reporting as a Serious Incident, Never Event, CQC Notification, NRLS Patient Safety Incident, RIDDOR Incident, etc. (see section 5.2 below);
- Advising Network Directors and Clinical Directors on compliance with this policy, relevant legislation and applicable standards;
- Providing guidance, support, advice and training for those staff with duties under this policy;
- Working with specialist managers and leads so they are fully engaged in the process set out in this policy to ensure a consistent approach to incident reporting, investigation, management and learning;
- Developing effective relationships with commissioners and regulators to provide confidence in the Trust's ability to report, investigate, manage and learn from incidents;
- Reviewing new serious incidents with the Director of Nursing and Quality and Medical Director and advising on a further level of investigation, taking action where necessary to address immediate concerns;
- Contributing to the development of thematic analysis, audits and quality surveillance in relation to incidents and learning from incidents.

4.4 **Network Directors/Clinical Directors** are responsible for:

- Ensuring compliance with this policy and other policies, systems and processes for the reporting, investigation, management and learning from incidents;

- Reviewing and approving Team Incident Reviews and Post Incident Reviews on behalf of the Network (this responsibility may be delegated to a deputy with approval of the Associate Director of Patient Safety and Quality Governance);
- Ensuring learning is identified and that recommendations are developed into action plans which are then implemented (including ensuring they are added to Datix, updated regularly and closed when complete);
- Ensuring the learning from incidents is implemented across the Network, making improvements to service and care delivery, and sharing learning with other Networks as appropriate;
- Commissioning thematic reviews and audit to provide assurance of the Network's compliance with policies, systems and processes for the reporting, investigation, management and learning from incidents, addressing or escalating matters of non-compliance.

Network Assurance and Governance Groups and Network Patient Safety/Quality/Risk Groups (or equivalent) will support Network Directors and Clinical Directors in the discharge of these duties by seeking assurance on the effective implementation of this policy.

Where an incident occurs in a corporate directorate, the relevant Director or Associate Director will undertake the duties above on behalf of their Directorate. References to Networks should then be interpreted to mean Directorate.

4.5 Senior Managers, managers and clinicians are responsible for ensuring compliance with this policy and other policies, systems and processes for the reporting, investigation, management and learning from incidents. Specifically they will be responsible for:

- Ensuring incidents are reported on Datix by their staff in a prompt fashion and no later than 24 hours following the incident;
- Taking immediate action following an incident to support people who are affected, preserving any evidence for future investigation and implementing any required immediate safety measures;
- Reviewing incident reports generated within Datix and completing a Local Investigation Review (within 7 working days) for Level 1 – 3 incidents and a 3 Day Review (within 3 working days) for Level 4 – 5 incidents;
- Ensuring staff are supported post incident, to include providing feedback on the outcome of an incident report and investigation;
- Ensuring compliance with the Trust Being Open Policy;
- Undertaking the role of, or support the appointed, investigation lead for a Team Incident Review or Post Incident Review;

- Ensuring the learning from incidents is implemented, making improvements to service and care delivery and ensuring their teams are fully engaged in the reporting and learning from incidents;
- Updating Datix at all stages with the progress of the incident investigation and implementation of recommendations and actions.

4.6 Investigation leads are responsible for ensuring their investigations are conducted in accordance with the policies, systems and processes for the investigation, management and learning from incidents and that they are completed within the required timescales.

An investigation lead may be either a senior manager or clinician from a Network or Corporate Directorate, or a specialist investigator from the Patient Safety and Quality Governance Department.

4.7 All staff have a responsibility to:

- Take responsibility for their own safety, and the safety of others in their care or affected by their actions;
- Report all incidents onto Datix within 24 hours;
- Take any immediate appropriate action to ensure safety (e.g. removal and quarantine of defective medical device);
- Cooperate with their manager and any other person conducting an investigation to the incident;
- Actively support the learning from incidents making improvements to service and care delivery.

4.8 The Board of Directors are ultimately accountable for ensuring the Trust provides safe and effective healthcare and will scrutinise incident performance data and challenge areas of non-compliance with legislation and standards. The Quality Committee of the Board will support the discharge of this duty by receiving a six monthly Serious Incident Report and the Quality and Safety Sub-committee will receive regular updates on incident performance.

4.9 The Serious Incident Advisory Group (SIAG) is a sub-group of the Quality and Safety Sub-committee and is responsible for control and assurance of the process relating to incidents. It will commission and review thematic reports, quality surveillance reports and a six-monthly Serious Incident Report. The SIAG will also oversee the process relating to Blue Light safety alerts.

- 4.10 The **Serious Incident Oversight Panel (SIOP)** is a sub-committee of SIAG and is responsible for ensuring the quality and effectiveness of the incident process, in particular for ensuring the quality of serious incident investigations and subsequent learning.
- 4.11 The **Executive Serious Incident Review Panel (SIRP)** is a sub-committee of SIAG and is responsible for reviewing all new serious incidents on a weekly basis (by examining the 3 Day Review) and commissioning a further level of investigation (i.e. no further action, additional clarifications, Team Incident Review or Post Incident Review). The Executive SI Review Panel may require an independent investigator be appointed, or that specific terms of reference be included in the investigation, or that specialist leads be involved in the investigation team (e.g. medicines management, health and safety, information governance, etc).
- 4.12 **Other committees and groups** will support the effective implementation of this policy as appropriate to their remit – for example the Trust groups covering health and safety, security management, medication safety, etc. will review the effective application of this policy and the analysis of incident data.

5.0 The Policy

5.1 Incident reporting

- 5.1.1 All incidents and near miss incidents are to be reported through the incident module of the Datix risk management system. This must be done within 24 hours of the incident occurring or within 24 hours of it being known an incident has occurred. It is the responsibility of all members of staff to ensure this is completed.
- 5.1.2 Incidents of a highly significant nature, including all Never Events and those that may attract immediate media attention, should also be reported to the Risk Helpdesk – 01772 773583 – during working hours (Monday to Friday, 9am to 4.30pm) or the Executive On-Call out of working hours.

The Associate Director of Patient Safety and Quality Governance will then be informed by the Risk Helpdesk and will ensure the Trust Executive Management Team and relevant departments (such as Communications) are appropriately advised. Out of hours, the Executive On-Call will be responsible for ensuring relevant notifications.

- 5.1.3 The Datix risk management system will be configured to issue notification emails to relevant specialists or senior managers based on the type of incident being reported. In addition, the Information Governance Department will be responsible for ensuring the Senior Information Risk Owner and Caldicott Guardian are advised of relevant incidents and the Finance Department will be responsible for ensuring the Local Counter Fraud Specialist is advised of relevant incidents.
- 5.1.4 In the event that the Datix system is unavailable for more than 24 hours, the Datix business continuity plan will be activated and paper records will be used (details will be communicated across the Trust by the Patient Safety and Quality Governance Department).
- 5.1.5 Managers are responsible for taking immediate action following an incident to support people who are affected, preserving any evidence for future investigation and implementing any required immediate safety measures.

5.2 External incident reporting

- 5.2.1 The Patient Safety and Quality Governance Department will be responsible for the external reporting of incidents as follows:
- Serious Incidents including Never Events will be reported using the NHS Strategic Executive Information System (STEIS) within 48 working hours of the incident occurring or the Trust becoming aware of the incident occurring;
 - Patient safety incidents will be uploaded to the NHS National Reporting and Learning System (NRLS) in accordance with required standards;
 - RIDDOR reportable incidents will be submitted to the Health and Safety Executive in accordance with legislative requirements;
 - Notification to the Care Quality Commission of specific incidents as required under the Health and Social Care Act 2012;
 - Notification to Monitor of specific incidents as required under the terms of the Foundation Trust licence;
 - Violence and aggression incidents will be reported to NHS Protect using the Security Incident Reporting System in accordance with national standards.
- 5.2.2 The Information Governance Department will be responsible for the external reporting of information governance incidents to the Department of Health and Information Commissioner's Office (ICO) in accordance with required standards and legislation.
- 5.2.3 The Property Services Department will be responsible for the external reporting of engineering, infrastructure and non-medical device defects and failures to the Department of Health.

- 5.2.4 The Education, Training and Professional Development Department will be responsible for notifying Health Education England (HEE) and its Local Education and Training Boards in relation to incidents involving their students.
- 5.2.5 The Pharmacy Department under the direction of the Chief Pharmacist (as Controlled Drugs Accountable Officer) will be responsible for reporting incidents involving controlled drugs to NHS England.
- 5.2.6 All staff are required to report incidents with a medicine or medical device to the MHRA using the Yellow Card Scheme (in addition to completing the Datix incident report): <https://www.gov.uk/report-problem-medicine-medical-device>.
- 5.2.7 The police will be notified as per the requirements of section 5.10 below.
- 5.2.8 It should be noted that a single incident may require multiple external reporting as above. In these cases the relevant departments should ensure they communicate with each other and that the Datix record is kept up to date.

5.3 Incident management

- 5.3.1 All incident reports submitted through Datix will be reviewed by the relevant manager. They are responsible for completing an investigation (see below) and updating the incident record within Datix. This must be done within 7 working days for level 1 – 3 incidents, 3 working days for level 4 – 5 incidents.
- 5.3.2 The Patient Safety and Quality Governance Department will perform a quality check on each incident record against a criteria approved by the Associate Director of Patient Safety and Quality Governance. Where a record fails this quality check it will be returned to the manager for correction, which must take place and be re-submitted within 5 working days.
- 5.3.3 Trust specialist managers or leads (e.g. Health & Safety, Security Management, Information Governance, etc.) will receive notification of incidents within their speciality and will take appropriate action as they see fit – however formal investigations must be conducted in accordance with this policy.

5.4 Incident investigation

- 5.4.1 Investigations carried out under this policy are conducted for the purposes of learning to prevent recurrence. They are not inquiries into how a person died (where applicable) as this is a matter for Coroners. Neither are they conducted

to hold any individual or organisation to account as other processes exist for that purpose including: criminal or civil proceedings, disciplinary procedures, employment law and systems of service and professional regulation, such as the Care Quality Commission and the Nursing and Midwifery Council, the Health and Care Professions Council, and the General Medical Council.

- 5.4.2 The scale and scope of the investigation should be proportionate to the incident to ensure resources are effectively used.
- 5.4.3 All relevant physical, scientific and documentary evidence must be obtained, reserved and securely stored as soon as possible following an incident to support the investigation. All investigative material should be retained and be readily available to share with an independent investigators or regulators if required.
- 5.4.4 Managers are responsible for conducting **Local Investigation Reviews** for Level 1 – 3 incidents within 7 working days. This form is completed within Datix. Managers should use this investigation process and tool to identify learning and to make changes with service and care delivery where identified to prevent recurrence and improve safety and quality.
- 5.4.5 The Incident Decision Tree (Appendix 8) should be used to promote fair and consistent staff treatment. In the very rare circumstances where a member of staff has committed a criminal or malicious act, staff should be advised at an early stage to enable them to obtain separate legal advice and/or representation. Where a disciplinary process is required their involvement in the incident investigation should cease and they should be investigated under the Disciplinary Policy (see Section 2.4). Information gained from the disciplinary investigation may be shared with the incident investigation.
- 5.4.6 For level 4 – 5 incidents managers must complete a **3 Day Review** investigation form (in Datix) within 3 working days. The Executive SI Review Panel will review completed 3 Day Review investigations (required for all level 4 – 5 incidents) and determine a further level of investigation if required – this could be:
- A **Team Incident Review (TIR)** which is a concise root cause analysis investigation;
 - A **Post Incident Review (PIR)** which is a comprehensive root cause analysis investigation.

TIR and PIR reports must be written and produced in an anonymised format – the Datix incident number and/or STEIS reference number will be used to identify the incident and cross reference to the Datix record.

- 5.4.7 Decisions from the Executive SI Review Panel will be communicated to the Network(s) or Head of Investigations as below:
- In the event of the investigation being allocated to a Network – the Network is responsible for appointing a lead investigator who is sufficiently senior

and trained in investigation techniques, agreeing terms of reference and completing the required investigation within the deadline (which will be 45 working days). For joint investigations across multiple Networks this is the responsibility of the Network where the incident occurred unless otherwise directed by the Executive SI Review Panel;

- In the event of the investigation being allocated to a specialist investigator from the Patient Safety and Quality Governance Department – the Head of Investigations is responsible for appointing a lead investigator from their team who is sufficiently competent, agreeing terms of reference and ensuring the investigation is completed within the deadline (which will be 45 working days). The relevant Network will be required to sign off the report and develop an action plan to address the identified recommendations.

5.4.8 All TIRs and PIRs are to be completed in accordance with the **Investigation Toolkit** produced by the Patient Safety and Quality Governance Department which is available on the Intranet.

5.4.9 For TIRs and PIRs those involved in the investigation process must not be involved in the direct care of those patients affected nor should they work directly with those involved in the delivery of that care. Demonstrating that an investigation will be undertaken objectively helps to provide those affected (including families/carers) with confidence that the findings of the investigation will be robust, meaningful and fairly presented.

5.4.10 The investigation lead should consider appointing an investigation team to support them in their work. This is particularly important for complex investigations where multi-disciplinary or expert input may be required.

5.4.11 The investigation lead should make it clear that the investigation itself is separate to any other legal and/or disciplinary process. There must be zero tolerance for inappropriate blame and those involved must not be unfairly exposed to punitive disciplinary action, increased medico-legal risk or any threat to their registration by virtue of involvement in the investigation process.

5.4.12 It is the responsibility of the investigation lead to develop robust recommendations that are based on the identified learning and which will seek to prevent recurrence of the incident and promote safety and quality. The investigation lead must consult all relevant persons in developing recommendations.

5.4.13 Upon completion of the investigation, the investigation report must be approved by the Network Director and Clinical Director, any learning identified and an action plan developed. This complete report must then be uploaded to Datix within the required deadline. For joint investigations this is the responsibility of the Network where the incident occurred.

Network Directors and Clinical Directors may delegate this sign off to a deputy/associate/assistant director however all nominated deputies must be notified to and approved by the Associate Director of Patient Safety and Quality Governance. In cases of patient safety incidents, at least one of the approvers must be a clinician.

- 5.4.14 Actions must be formulated by those who have responsibility for implementation, delivery and financial aspects of any actions. Networks must ensure all actions from the approved investigation report are added to Datix. For joint investigations, this is the responsibility of the Network where the incident occurred. The responsible action lead must then update Datix on a regular basis until the action is deemed complete. Networks must establish a process to monitor the completion of actions within set timescales.
- 5.4.15 Where this is a significant disagreement between the recommendations proposed by the Investigation Lead and the action plan developed by the Network, then the Serious Incident Oversight Panel will determine the final action plan on behalf of the Trust.
- 5.4.16 Serious incident investigation reports will be submitted to the appropriate commissioner for their review and quality assurance in accordance with the NHS England Serious Incident Framework. Where commissioners require further assurances the Patient Safety and Quality Governance Department will liaise with the Network to provide additional details which will require a Network Director or Clinical Director (or nominated deputy as above) sign off.
- 5.4.17 Commissioners may require that all actions are complete before the above sign off is accepted.
- 5.4.18 The Serious Incident Oversight Panel will provide a quality assurance process for investigation reports and commissioner responses. The SIOP may require further clarifications or amendments to reports and recommendations/actions from Networks.
- 5.4.19 Process charts are included at appendix 1 and 2.

5.5 Regulatory investigations

- 5.5.1 NHS England may commission an independent investigation into cases of homicide caused by a patient under the care of mental health services. The Associate Director of Patient Safety and Quality Governance will coordinate the Trust's involvement in these investigations.
- 5.5.2 The Information Governance Team will coordinate any subsequent investigations by the Information Commissioner.

- 5.5.3 The Associate Director of Patient Safety and Quality Governance will coordinate any subsequent investigations by the Health and Safety Executive (HSE), Care Quality Commission (CQC), Monitor or other regulators and commissioners.

5.6 Coroners inquests

- 5.6.1 The Coroner is notified of all deaths. When a death is unexpected, violent or unnatural, the Coroner will decide whether to hold a post-mortem and, if necessary, an inquest. When a person dies in the custody of the legal authorities, including detention under Mental Health Act, an inquest must be held. The Coroner's court is a court of law, and accordingly the Coroner may summon witnesses to attend and give evidence.
- 5.6.2 Where a coroner's verdict is not known at the time of the investigation report being completed, the final investigation report will be submitted within the appropriate timescale and not delayed in order to incorporate the coroner's verdict. It must be made clear in the report that a coroner's verdict is awaited. Once the verdict is available, this must be recorded within Datix. If the verdict presents issues not covered in the final report, then the Trust will revise the report in order to incorporate these issues.
- 5.6.3 Investigation leads must be mindful that the coroner is likely to request a copy of any investigation report and that they may be called as a witness at the Inquest.
- 5.6.4 The Inquest Policy sets out how the Trust will engage with Coroners inquests.

5.7 Safeguarding incidents

- 5.7.1 Safeguarding incidents that proceed to a Serious Case Review, Domestic Homicide Review or similar follow a different investigation and approval process which is detailed at appendix 3. In these cases the completed safeguarding investigation report will take the place of the internal Trust investigation report unless otherwise agreed by the Associate Director of Patient Safety and Quality Governance and Assistant Director of Safeguarding. However the initial incident reporting and subsequent learning follows the same incident process.

5.8 Infection control incidents

- 5.8.1 Certain infection control incidents may require the completion of a Post Infection Review in addition, or as an alternative to, a Team Incident Review or Post Incident Review. The Patient Safety and Quality Governance Department will coordinate all Post Infection Reviews. However the initial reporting and subsequent learning follows the same incident process.

5.9 Deaths in custody

- 5.9.1 All deaths in custody – including those of people detained under the Mental Health Act – will be subject to an investigation. Where the patient is in police or prison custody the death will be referred by that organisation to the Prison and Probation Ombudsmen (PPO) who will conduct an investigation. The Trust, in addition to its own investigation, will fully support the PPO investigation.

5.10 Police involvement

- 5.10.1 The police should be notified of all incidents where there is:

- evidence or suspicion that the actions leading to harm (including acts of omission) were reckless, grossly negligent or wilfully neglectful;
- evidence or suspicion that harm/adverse consequences were intended;
- a suspicious or accidental death.

Guidance on notifying the police can be obtained from the Trust Security Manager.

- 5.10.2 Where the police conduct an investigation into an incident the Trust's own investigation would normally continue. However, the police may request that the Trust's own investigations are suspended until the police investigation is complete. In these cases the lead investigator must inform the Associate Director of Patient Safety and Quality Governance and must keep in regular contact with the police lead investigator to agree when the Trust investigation may commence.

5.11 Trade union involvement

- 5.11.1 Trade Union Health and Safety Representatives have the right to access information regarding incidents and investigations which may potentially affect the staff they represent. While there is a requirement for consultation with Trade Union Health and Safety Representatives, it is good practice to actively involve them in the initial undertaking and subsequent reviews of incidents and investigations for their area.

5.12 Learning from incidents

- 5.12.1 The overall aim and key objective of investigating incidents is to identify if there are any areas of learning for the organisation. Actions will be developed by the Network as stated above as part of the investigation report that ensures the learning is turned into tangible improvements in care and service delivery.
- 5.12.2 Managers conducting Local Investigation Reviews and 3 Day Reviews should ensure learning is shared within their team. This must include providing feedback to the person who recorded the incident as this encourages further incident reporting and learning. Additionally, managers should consider whether the learning could apply to other teams and Networks in which case this should be raised through their senior manager.
- 5.12.3 Whilst lead investigators for TIRs and PIRs should identify recommendations the responsibility for identifying lessons learned as to and how the learning from their investigations will be shared with the team, Network and wider Trust (if appropriate) lies with the Network. Lead investigators must consult with clinicians and managers within the Network on how this can be best achieved. The methods of sharing the learning must be specifically detailed on the action plan.
- 5.12.4 Network Directors and Clinical Directors are responsible for ensuring the learning from incidents is implemented across the Network, making improvements to service and care delivery, and sharing learning with other Networks as appropriate
- 5.12.5 The process of initiating and cascading Trust-wide Blue Light and Green Light safety alerts, and external alerts, is detailed in the Safety Alerts Policy.
- 5.12.6 Network Directors and Clinical Directors are responsible for commissioning thematic reviews and audit to provide assurance of the Network's compliance with policies, systems and processes for the reporting, investigation, management and learning from incidents, and for addressing or escalating matters of non-compliance.
- 5.12.7 The Executive Director of Nursing and Quality and the Medical Director are responsible for commissioning and leading the development of thematic analysis and quality surveillance in relation to incidents and learning from incidents. The Associate Director of Patient Safety and Quality Governance will support this by developing a mechanism to theme incident data and triangulate this data with other risk management data (such as complaints, claims, risk registers, Quality SEEL assessments, etc).
- 5.12.8 The Associate Director of Patient Safety and Quality Governance will develop a matrix highlighting all thematic reports and quality surveillance conducted at

a Trust level. The SIAG will oversee the process of Trust level thematic reports and quality surveillance and may commission specific or ongoing reports.

5.13 Being Open (Duty of Candour)

5.13.1 The Trust has a duty to be open with patients, their relatives and carers when harm has occurred – this duty is detailed in the Being Open Policy and must be applied in all circumstances.

5.13.2 Early, meaningful and sensitive engagement with affected patients and/or their families/carers should be established from the point at which an incident is identified, throughout the investigation, report formulation and subsequent action planning through to closure of the investigation process. A specific person should be assigned to engage with the family to provide a single point of contact. This will normally be the lead investigator.

5.13.3 For investigations that may take place over a long period of time such as suicide and homicide investigations, contact details of any patients, relatives, carers and victims should be maintained, where possible, to enable future contact to discuss the outcome of investigations.

5.13.4 Whilst the Being Open Policy and Duty of Candour relate to patient safety incidents, the Trust expects the same principles to be applied to other incidents such as staff incidents.

5.14 Support for staff

5.14.1 The Trust recognises that staff, either as individuals or working as part of a team, who are involved in an incident may be affected by the event both professionally and/or on a personal level. The Trust is committed to supporting staff through these challenging situations and acknowledges the need to ensure timely and appropriate support. For further details please refer to the Procedure for Supporting Staff following Traumatic/Stressful Incidents which must be applied in all circumstances.

6.0 Training

6.1 The Associate Director of Patient Safety and Quality Governance will be responsible for the development and delivery of a training programme to support the effective implementation of this policy which will include:

- Incident reporting training for all staff;

- Incident management training for all managers;
- Incident investigation training for managers appointed as investigators to include root cause analysis techniques;
- Additional specialist incident training as required.

7.0 Monitoring

Standard	Time frame/format	How	Whom
<i>Review of Incident Reports</i>	<i>Within 3 or 7 working days of the incident occurring depending on level</i>	<i>Review of all incident reports and completion of investigation</i>	<i>Managers</i>
<i>Review of 3 Day Reviews</i>	<i>Weekly</i>	<i>Review of all 3 Day Reviews and decision on further investigations</i>	<i>Managers, Executive SI Review Panel</i>
<i>Review of TIRs/PIRs</i>	<i>As required</i>	<i>Review of all TIRs/PIRs to ensure quality standards are achieved</i>	<i>Network/Clinical Directors and SIOP</i>
<i>Thematic reports and quality surveillance</i>	<i>As required</i>	<i>Review of incident data to identify trends, hot spots and compliance with standards</i>	<i>Network/Clinical Directors and SIAG</i>
<i>SI Report</i>	<i>Six-monthly</i>	<i>Review of serious incident data to identify trends, hot spots and determine actions to improve safety</i>	<i>SIAG/Quality Committee</i>

7.0 References

NHS England (2015). Serious Incident Framework. Available at <http://www.england.nhs.uk/wp-content/uploads/2015/04/serious-incident-framework-upd.pdf>

NHS England (2015). Never Event Framework. Available at <http://www.england.nhs.uk/wp-content/uploads/2015/04/never-events-policy-framework-apr.pdf>

National Patient Safety Agency (2009). Being open: communicating patient safety incidents with patients, their families and care. Available at: <http://www.nrls.npsa.nhs.uk/resources/collections/being-open/?entryid45=83726>

National Patient Safety Agency (2004). Seven Steps to Patient Safety. Available at: <http://www.nrls.npsa.nhs.uk/resources/?entryid45=59787&q=0%acseven+steps+to+patient+safety%ac>

Care Quality Commission (March 2015). Fundamental Standards on Quality and Safety. Available at <http://www.cqc.org.uk/content/regulations-service-providers-and-managers>

Care Quality Commission (March 2015). Registrations and notifications. Available at <http://www.cqc.org.uk/content/registration-notifications-fees>

Work related deaths: A protocol for liaison (England and Wales). Available at: <http://www.hse.gov.uk/pubns/wrdp1.pdf>

Memorandum of Understanding (MOU) investigating patient safety incidents involving unexpected death and serious untoward harm: a protocol for liaison and effective communications between the National Health Service, Association of Chief Police Officers and Health and Safety Executive. Available at: http://www.dh.gov.uk/PublicationsAndStatistics/Publications/PublicationsPolicyAndGuidance/PublicationsPolicyAndGuidanceArticle/fs/en?CONTENT_ID=4141440&chk=yb8CgY

NHS Connecting for Health (2010). Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents. Available at <http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/suichecklist.pdf>

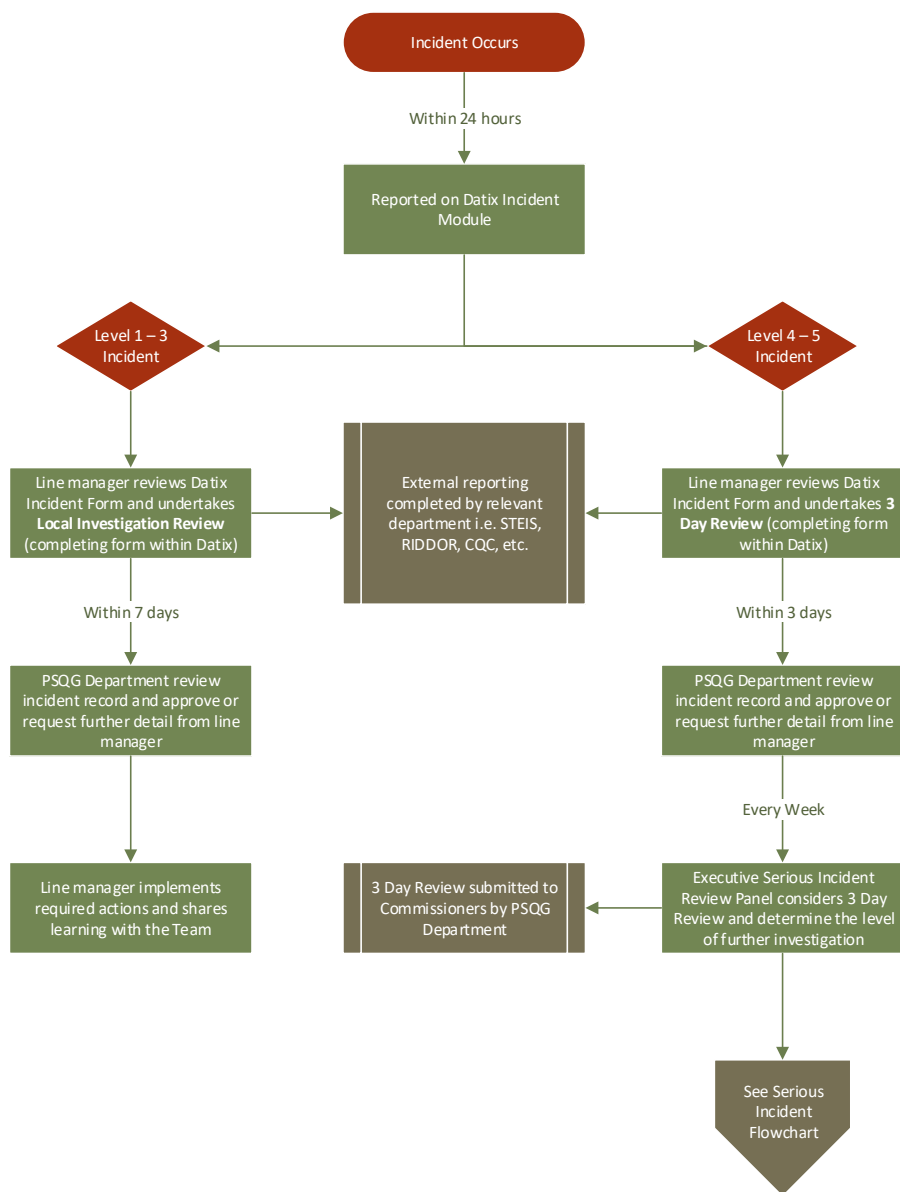
Health and Safety Executive (2013). Reporting injuries, diseases and dangerous occurrences in health and social care. Available at: <http://www.hse.gov.uk/pubns/hsis1.pdf>

NHS England (2015). Standard Operating Procedure for all organisations to use the CD reporting website. Available at: <http://www.cqc.org.uk/content/law-and-guidance-managing-controlled-drugs>

Appendix 1 – Incident Reporting and Management Process

Incident Reporting Process

For further details please refer to the Trust Incident Policy

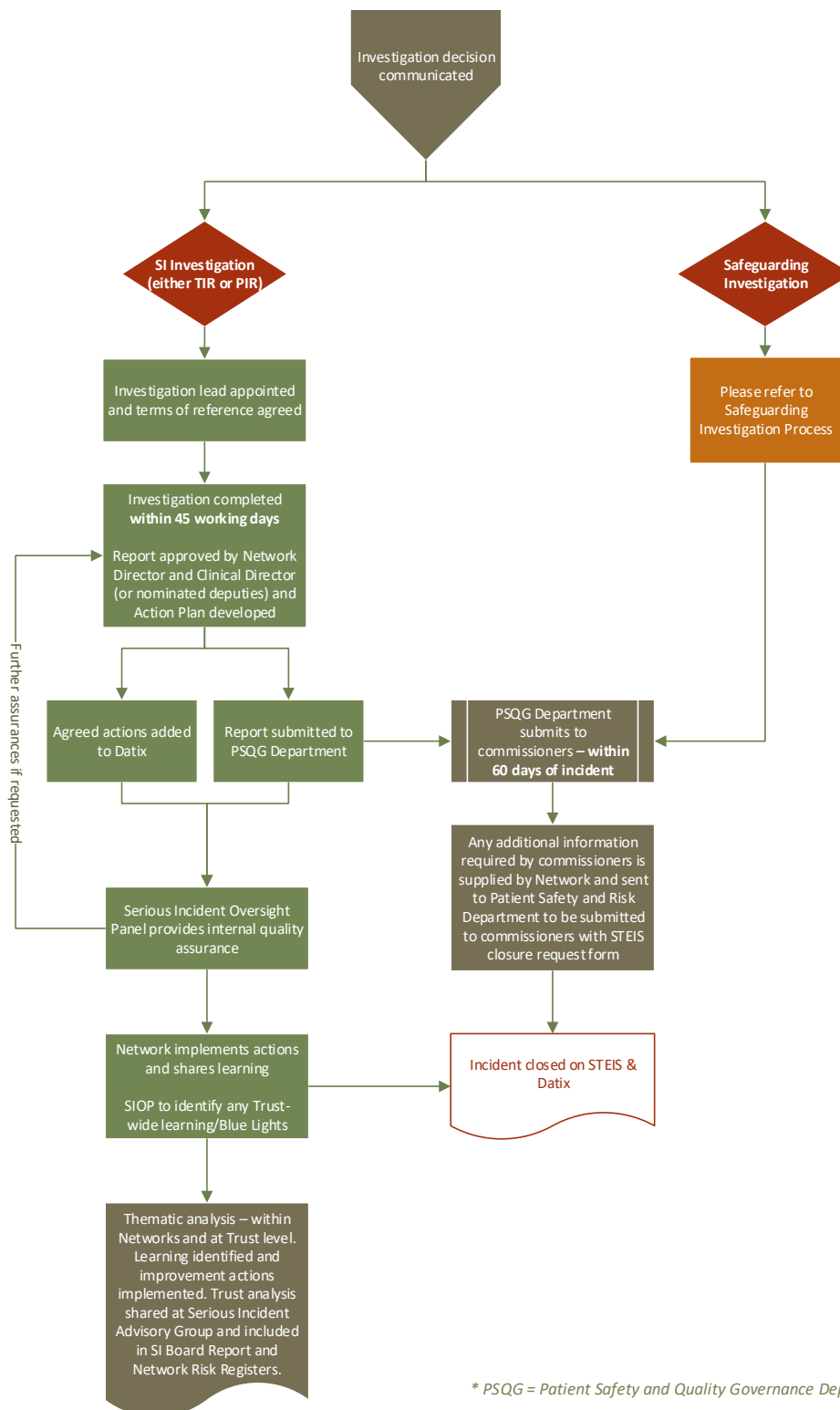


* PSQG = Patient Safety and Quality Governance Department

Appendix 2 – Serious Incident Investigation Process

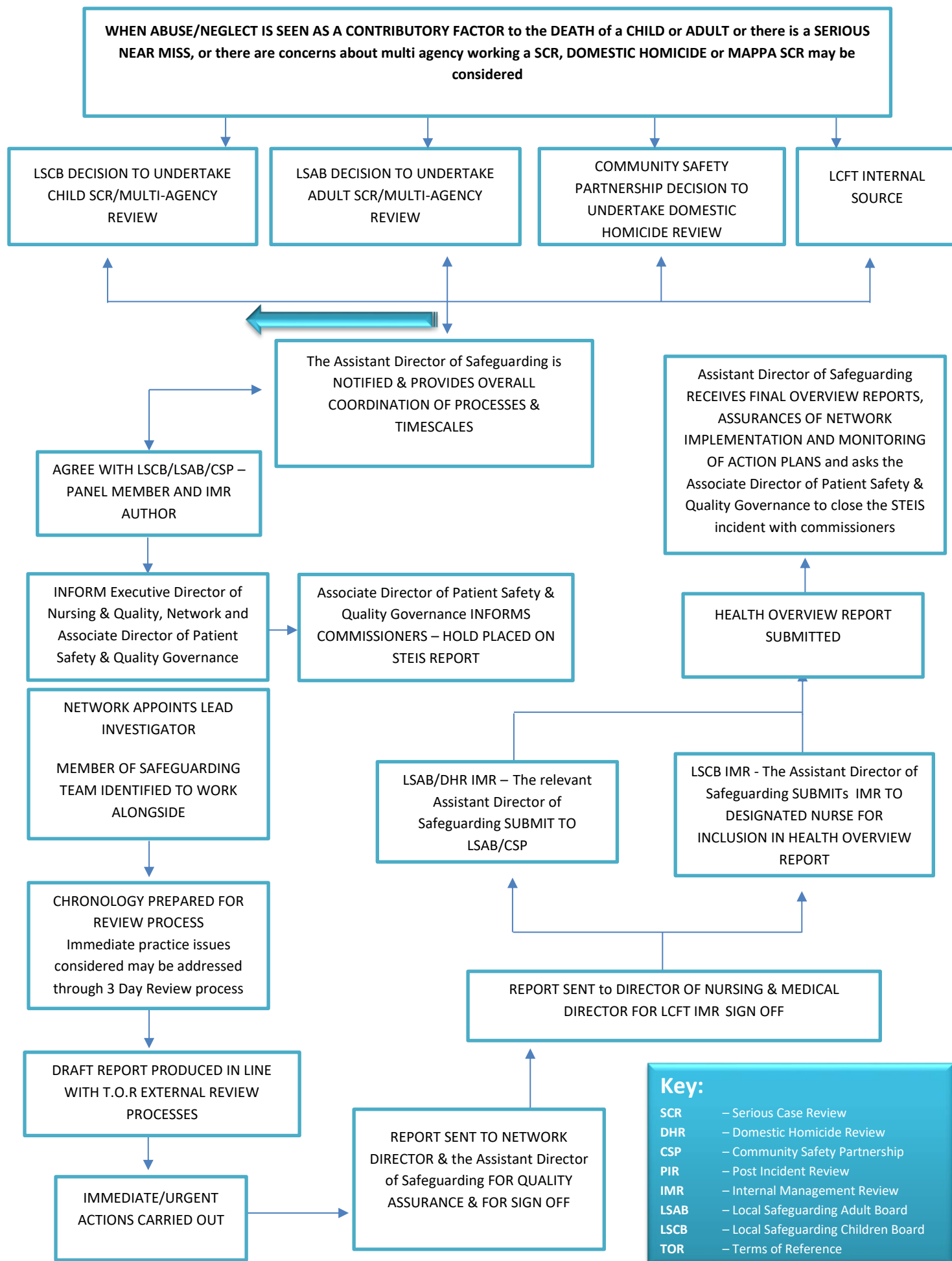
Serious Incident Process

For further details please refer to the Trust Incident Policy



* PSQG = Patient Safety and Quality Governance Department

Appendix 3 – Safeguarding Incident Investigation Process



Appendix 5 – Incident Level Guidance

The incident level relates to the actual harm suffered from the incident or the potential harm if a near miss incident

	Level 1 INSIGNIFICANT	Level 2 LOW	Level 3 MODERATE	Level 4 SEVERE	Level 5 CATASTROPHIC
	Managers must complete the Local Investigation Review section on Datix			Managers must complete a 3 Day Review on Datix – the Executive SI Review Panel will then decide on a TIR or PIR	
Incidents resulting in harm to people (patients, staff or public)	Incident resulting in no actual harm	Incident resulting in minor harm (e.g. first aid assistance) or absence from work of under 7 days	Incident resulting in moderate harm (e.g. A&E assessment) or absence from work of over 7 days	Incident resulting in severe harm (e.g. fractures or long term conditions/disability)	Death of a patient, staff member or member of the public as a result of an incident
Patient care <i>Including all clinical interventions, outcomes and patient experience</i>	Patient care incident with no actual harm or negative clinical outcome	Minor patient care incident or poor clinical outcome (i.e. readily resolvable)	Patient care incident requiring moderate medical intervention for recovery	Severe patient care incident requiring complex medical intervention and/or long term recovery or causing long term conditions/disability (including Grade 3 and 4 Pressure Ulcers)	Catastrophic patient care incident resulting in death
Violence and aggression <i>Including sexual, racial and discriminatory violence and aggression</i>	Aggression (verbal and physical) not directed at individuals and with no harm to people or damage to property	Physical assault resulting in minor harm to people (e.g. first aid assistance) or property Minor verbal aggression	Physical assault resulting in moderate harm to people (e.g. A&E assessment) property Moderate verbal aggression	Physical assault resulting in severe harm to people (e.g. fractures or long term conditions/ disability) to property (including all attempted or actual rape and hate crime) Severe verbal aggression including racial abuse, discrimination and sexual advances	Death of a patient, staff member or member of the public as a result of violence and aggression (including all homicides)
Self-harm	Indications of self-harm	Minor incidents of self-harm (requiring first aid intervention)	Moderate incidents of self-harm (requiring A&E assessment)	Severe incidents of self-harm (such as life threatening incidents or those resulting in permanent harm) (including serious inpatient attempted suicides/ligatures)	Death of a patient from self-harm (including all suicides)

	Level 1 INSIGNIFICANT	Level 2 LOW	Level 3 MODERATE	Level 4 SEVERE	Level 5 CATASTROPHIC
	Managers must complete the Local Investigation Review section on Datix			Managers must complete a 3 Day Review on Datix – the Executive SI Review Panel will then decide on a TIR or PIR	
Medication	Medication incident with no actual or potential harm	Medication incident causing minor harm and no breach of policy	Medication incident causing moderate harm and is a breach of policy	Medication incident causing severe harm and is a breach of policy and legislation (including causing any long term condition/disability)	Medication incident causing death
AWOL, abscond and escape	Attempted AWOL or abscond	AWOL/abscond – patient assessed as minor risk to self or others Attempted escape from ward	AWOL/abscond – patient assessed as moderate risk to self or others Patient escape from ward	AWOL/abscond – patient assessed as severe risk to self or others or patient AWOL/abscond from low or medium secure services Patient escape from low secure	Patient escape from medium secure wards
Information governance	Insignificant breach of confidentiality or health records error – no personal or clinical data or confidential data lost, no media interest or no actual or potential harm from breach/error, security controls are in place to mitigate the risk Scale: less than 10 individuals affected	Minor breach of confidentiality or health records error – limited clinical information is at risk, basic demographic personal data has been lost or confidential data lost, no media interest or low harm from breach/error Scale: 11-100 individuals affected	Moderate breach of confidentiality – limited personal or clinical data or confidential data lost, potential media interest or moderate harm from breach/error Scale: 101 – 1000 individuals affected	Severe breach of confidentiality resulting in the loss of detailed personal/clinical data or confidential and particularly sensitive data and/or media interest or individual/s affected are likely to suffer significant distress or embarrassment from breach/error Scale: 1,001– 5000 individuals affected	Catastrophic breach of confidentiality resulting in major loss of sensitive personal data and media interest, the incident has incurred or risked incurring a clinical untoward incident Scale: 5001 + individuals affected
Fire	Fire alarm false activation	Small fire, contained and extinguished without Fire Service assistance, no disruption to service delivery, minor injury to patients, staff or the public	Moderate fire requiring Fire Service assistance, moderate damage to property and disruption to service delivery, moderate injury to patients, staff or the public	Severe fire requiring Fire Service assistance, severe damage to property and disruption to service delivery, severe injury to patients, staff or the public	Catastrophic fire requiring Fire Service assistance, catastrophic damage to property and disruption to service delivery, death to patients, staff or the public
Disruption to service and care delivery <i>Including security, estates and IM&T issues</i>	Disruption to services for a brief period time – no impact on patient care or essential functions	Minor disruption to services, quickly resolved with no medium or long term impact	Moderate disruption to services, resolved within a shift or day, with no long term impact, non-compliance with Trust Policy	Severe disruption to services, long term impact on services, damage to reputation, non-compliance with standards or legislation (including admission of minors to adult wards)	Catastrophic disruption to services requiring implementation of emergency plans (including major incidents or business continuity incidents)

Appendix 6 – Externally Reported Incidents (STEIS/RIDDOR etc.)

This appendix details those incidents that are required to be reported externally by notification recipient – it should be considered that a single incident may be subject to more than one external notification.

Commissioners: Strategic Executive Information System (STEIS)

In broad terms, serious incidents are events in health care where the potential for learning is so great, or the consequences to patients, families and carers, staff or organisations are so significant, that they warrant using additional resources to mount a comprehensive response. Serious incidents can extend beyond incidents which affect patients directly and include incidents which may indirectly impact patient safety or an organisation's ability to deliver ongoing healthcare.

The Patient Safety and Quality Governance Department will undertake all STEIS reporting. This reporting must be completed within 48 hours of the incident occurring, or 48 hours of the Trust being made aware of an incident.

Serious Incidents in the NHS include:

- Acts and/or omissions occurring as part of NHS-funded healthcare (including in the community) that result in:
 - Unexpected or avoidable death of one or more people. This includes suicide/self-inflicted death, deaths in custody and homicide by a person in receipt of mental health care (to include a patient who has been discharged within the preceding 6 months);
 - Unexpected or avoidable injury to one or more people that has resulted in serious harm (including Grade 3 and 4 pressure ulcers that have been deemed as occurring in Trust care and avoidable);
 - Unexpected or avoidable injury to one or more people that requires further treatment by a healthcare professional in order to prevent the death of the service user or serious harm;
 - Actual or alleged abuse; sexual abuse, physical or psychological ill-treatment, or acts of omission which constitute neglect, exploitation, financial or material abuse, discriminative and organisational abuse, self-neglect, domestic abuse, human trafficking and modern day slavery where:
 - healthcare did not take appropriate action/intervention to safeguard against such abuse occurring (such as failing to effectively care plan, share information or follow safe recruitment policies); or
 - where abuse occurred during the provision of NHS-funded care.
- A Never Event (see Appendix 7);

- An incident (or series of incidents) that prevents, or threatens to prevent, an organisation's ability to continue to deliver an acceptable quality of healthcare services, including (but not limited to) the following:
 - Failures in the security, integrity, accuracy or availability of information often described as data loss and/or information governance related (see the Information Governance section below);
 - Property damage;
 - Security breach/concern (including a patient who is absent without leave (AWOL) and poses a significant risk to themselves or the public);
 - Incidents in population-wide healthcare activities like screening and immunisation programmes where the potential for harm may extend to a large population;
 - Inappropriate enforcement/care under the Mental Health Act (1983) and the Mental Capacity Act (2005) including Mental Capacity Act, Deprivation of Liberty Safeguards (MCA DOLS);
 - Systematic failure to provide an acceptable standard of safe care (this may include incidents, or series of incidents, which necessitate ward/ unit closure or suspension of services); or
 - Activation of Major Incident Plan (by provider, commissioner or relevant agency).
- Major loss of confidence in the service, including prolonged adverse media coverage or public concern about the quality of healthcare or an organisation.

The reporting portal is at: <http://nww.steis.doh.nhs.uk/steis/steis.nsf/main?readForm>.

National Reporting and Learning System (NRLS)

The Trust is required to report patient safety incidents to the National Reporting and Learning System. The Patient Safety and Quality Governance Department will undertake all NRLS reporting by means of a data upload from the Datix risk management system. This will be done on a weekly basis using the NRLS web site: <https://report.nrls.nhs.uk/nrlsreporting>.

NHS Protect: Security Incident Reporting System (SIRS)

The SIRS system is operated by NHS Protect to nationally report security and violence and aggression incidents. The Patient Safety and Quality Governance Department will undertake all SIRS reporting.

Care Quality Commission (CQC)

The Trust is required to notify the Care Quality Commission (CQC) of specific changes in circumstances and of specific incidents as required by the Health and Social Care Act 2012. The Patient Safety and Quality Governance Department will undertake all CQC reporting in accordance with the Trust protocol: *A system for the management of statutory notifications as required by the Health and Social Care Act 2008 (COR020)* – many incidents are reported to the CQC through the NRLS system however certain incidents require the submission of a separate form:

- Deaths (all services) and unauthorised absences (secure services) of people who are detained or liable to be detained under the Mental Health Act 1983;
- Placement of children or young people on an adult psychiatric ward.

Notification forms can be accessed at: <http://www.cqc.org.uk/content/notifications>.

Health and Safety Executive (HSE): Reporting of Injuries Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR)

The Trust is required to report certain work related accidents to the Health and Safety Executive (HSE):

- All deaths to employees and non-employees, with the exception of suicides, must be reported if they arise from a work-related accident, including an act of physical violence to a worker;
- Specified injuries to employees such as:
 - fractures, other than to fingers, thumbs and toes;
 - amputations;
 - any injury likely to lead to permanent loss of sight or reduction in sight;
 - any crush injury to the head or torso causing damage to the brain or internal organs;
 - serious burns (including scalding) which:
 - covers more than 10% of the body;
 - causes significant damage to the eyes, respiratory system or other vital organs;
 - any scalping requiring hospital treatment;
 - any loss of consciousness caused by head injury or asphyxia;
 - any other injury arising from working in an enclosed space which:
 - leads to hypothermia or heat-induced illness ;
 - requires resuscitation or admittance to hospital for more than 24 hours;
- Accidents must be reported where they result in an employee or self-employed person being away from work, or unable to perform their normal work duties, 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;

- Accidents to members of the public or others who are not at work (such as patients) must be reported if they result in an injury and the person is taken directly from the scene of the accident to hospital for treatment to that injury. Examinations and diagnostic tests do not constitute 'treatment' in such circumstances. There is no requirement to report incidents where people are taken to hospital purely as a precaution when no injury is apparent. If the accident occurred at a hospital, the report only needs to be made if the injury is a 'specified injury' (see above);
- Diagnoses of certain occupational diseases to employees where these are likely to have been caused or made worse by their work: These diseases include:
 - carpal tunnel syndrome;
 - severe cramp of the hand or forearm;
 - occupational dermatitis;
 - hand-arm vibration syndrome;
 - occupational asthma;
 - tendonitis or tenosynovitis of the hand or forearm;
 - any occupational cancer;
 - any disease attributed to an occupational exposure to a biological agent (such as contracting a blood borne virus through work);
- Dangerous occurrences which are certain, specified, near-miss events. Not all such events require reporting. There are 27 categories of dangerous occurrences that are relevant to most workplaces, for example:
 - the collapse, overturning or failure of load-bearing parts of lifts and lifting equipment;
 - any accident or incident which results or could have resulted in the release or escape of a biological agent likely to cause severe human infection or illness – this includes an employee receiving a sharps injury contaminated with a known blood borne virus risk;
 - the accidental release of any substance which could cause injury to any person.

The Patient Safety and Quality Governance Department will undertake all RIDDOR reporting. RIDDOR reports must be submitted without delay, or within 15 days for over 7 day absences. The Health and Safety Executive online reporting portal is at: <http://www.hse.gov.uk/riddor/report.htm>.

Information Commissioner (ICO)

The Trust is required to report certain Information Governance (IG) incidents including any incident which involves actual or potential failure to meet the requirements of the

Data Protection Act 1998. This includes unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people's privacy and, breach of the Common Law of Confidentiality.

The IG Department receive Datix alerts for IG incidents. If the incident has been logged as a serious incident or there is a query about the severity of the incident, the IG Department will conduct an additional assessment using the IG Incident Reporting Tool for Serious Incidents to determine if the incident should be reported to the ICO. The IG Incident Reporting Tool for Serious Incidents considers the scale of the incident and the sensitivity factors.

A serious IG incident assessed as level 0 or level 1 is expected to be managed in accordance with local procedures. However a serious IG incident assessed at level 2 or above is reported to the ICO (in addition to becoming Serious Incident - see above. In some cases the ICO will undertake further investigation of the incident with the Trust. Any incidents investigated by the ICO could result in regulatory action and / or a monetary penalty.

The Information Governance Department will undertake all ICO information governance reporting and are responsible for liaising with the ICO and updating the progress of level 2 or above serious IG incidents on the IG Incident Reporting Tool.

Department of Health

Where incidents relate to a defect or failure involving engineering plants, infrastructure and/or non-medical devices, a defect and failure report will be submitted to the Department of Health via the defect and failure reporting portal <http://efm.hscic.gov.uk>. The Property Services Department will be responsible for all such notifications.

Health Education England

Health Education England (HEE) and its Local Education and Training Boards are responsible for the quality of the education and training provided to medical, nursing, dental and Allied Health Professionals (AHP) students and others, and training grade doctors. These students may be involved in serious incidents and HEE have a duty of care to them. The Education, Training and Professional Development Department will be responsible for notifying them on incidents involving their students.

Monitor

The Trust is required to inform Monitor about relevant serious incidents (i.e. any incidents which may reasonably be regarded as raising potential concerns over compliance with the Trust licence). The Associate Director of Patient Safety and Quality Governance will undertake such notifications under the direction of the Executive Director of Nursing and Quality.

Medicines and Healthcare products Regulatory Agency (MHRA)

The Trust must report suspected problems ('adverse incidents') with a medicine or medical device to the MHRA using the Yellow Card Scheme as soon as possible if:

- A medicine causes side effects;
- Someone's injured by a medical device, either because its labelling or instructions aren't clear, it's broken or has been misused;
- A patient's treatment is interrupted because of a faulty device;
- Someone receives the wrong diagnosis because of a medical device;
- A medicine doesn't work properly;
- A medicine is of a poor quality;
- A medicine or medical device is fake or counterfeit.

It is the responsibility of each member of staff to complete the report in addition to completing the Datix incident report using the online notification form: <https://www.gov.uk/report-problem-medicine-medical-device>.

Public Health England

Public Health England (PHE) Screening and Immunisation Leads, based within NHS England Sub-regions, have a system leadership role for screening and immunisation programmes. They have a responsibility to support the oversight and management of incidents which occur within these programmes and will liaise with other PHE experts to ensure that the investigation and response to an incident is managed appropriately.

PHE also has a broader role in supporting the management of serious incidents that occur within other NHS services, where there is a potential for the incident to have adversely affected the health of a wider population. Such incidents may include decontamination failures; inadvertent contact on NHS premises of patients and staff with someone with a transmissible infectious disease such as measles or TB; outbreaks of health care associated infections; the finding of a Health Care Worker infected with a blood borne virus; failure of microbiological laboratory practice; release/widespread exposure to harmful chemicals or a source of radiation.

Where the potential exists for the health of a wider group of people to be adversely affected by an incident in the NHS, the Trust must contact the relevant Public Health

England Centre through their Health Protection Team and involve PHE as part of the local incident control team. This contact will be organised through the Patient Safety and Quality Governance Department.

NHS England

The Trust's nominated Controlled Drugs Accountable Officer (CDAO) is responsible for notifying NHS England of all incidents involving controlled drugs. The Pharmacy Department under the direction of the Chief Pharmacist (as Controlled Drugs Accountable Officer) will be responsible for reporting these incidents using the online reporting portal: www.cdreporting.co.uk.

Appendix 7 – Never Events

Never Events are a particular type of serious incident that are wholly preventable and where guidance or safety recommendations that provide strong systemic protective barriers are available at a national level, and should have been implemented by all healthcare providers.

The following is a summary list of never events that will be applicable to mental health and community health services:

Never Event	Guidance
Chest or neck entrapment in bedrails	Entrapment of a patient's chest or neck within bedrails, or between bedrails, bedframe or mattress, where the bedrail dimensions or the combined bedrail, bedframe and mattress dimensions do not comply with Medicines and Healthcare products Regulatory Agency (MHRA) guidance.
Failure to install functional collapsible shower or curtain rails	Involves either; <ul style="list-style-type: none"> • Failure of collapsible curtain or shower rails to collapse when an inpatient suicide is attempted/successful; • Failure to install collapsible rails and an inpatient suicide is attempted/successful using these non-collapsible rails.
Falls from poorly restricted windows	A patient falling from poorly restricted window. <ul style="list-style-type: none"> • Applies to windows "within reach" of patients. This means windows (including the window sill) that are within reach of someone standing at floor level and that can be exited/fallen from without needing to move furniture or use tools to assist in climbing out of the window; • Includes windows located in facilities/areas where healthcare is provided and where patients can and do access; • Includes where patients deliberately or accidentally fall from a window where a restrictor has been fitted but previously damaged or disabled, but does not include events where a patient deliberately disables a restrictor or breaks the window immediately before the fall; • Includes where patients are able to deliberately overcome a window restrictor by hand or using commonly available flat bladed instruments as well as the 'key' provided.
Mis – selection of a strong potassium containing solution	Mis - selection refers to when a patient intravenously receives a strong potassium solution rather than an intended different medication.

Never Event	Guidance
Mis – selection of high strength midazolam during conscious sedation	<p>Mis - selection refers to</p> <ul style="list-style-type: none"> When a patient receives an overdose due to the selection of a high strength midazolam preparation (5mg/ml or 2mg/ml) rather than the 1mg/ml preparation, in a clinical area performing conscious sedation; Excludes clinical areas where the use of high strength midazolam is appropriate. These are generally only in general anaesthesia, intensive care, palliative care, or where its use has been formally risk assessed within an organisation.
Misplaced naso- or oro-gastric tubes	<p>Misplacement and use of a naso- or oro-gastric tube in the pleura or respiratory tract where the misplacement of the tube is not detected prior to commencement of feeding, flush or medication administration.</p>
Overdose of Insulin due to abbreviations or incorrect device	<p>Overdose refers to:</p> <ul style="list-style-type: none"> When a patient receives a tenfold or greater overdose of insulin because a prescriber abbreviates the words 'unit' or 'international units' , despite the care setting having an electronic prescribing system in place; When a health care professional fails to use a specific insulin administration device i.e. does not use an insulin syringe or insulin pen to measure insulin.
Overdose of methotrexate for non-cancer treatment	<p>Overdose refers to when a patient receives methotrexate, via any route, for non-cancer treatment which results in more than the intended weekly dose being taken, despite the care setting having an electronic prescribing and administration system , or in primary care an electronic prescribing and dispensing system, in place</p>
Scalding of patients	<p>Patient being scalded by water used for washing/bathing. Excludes scalds from water being used for purposes other than washing/bathing (e.g. from kettles).</p>
Wrong route administration of medication	<p>The patient receives one of the following:</p> <ul style="list-style-type: none"> Intravenous chemotherapy administered via the intrathecal route; Oral/enteral medication or feed/flush administered by any parenteral route; Intravenous administration of a medicine intended to be administered via the epidural route.

Appendix 8 – Incident Decision Tree

Work through the tree separately for each individual involved

