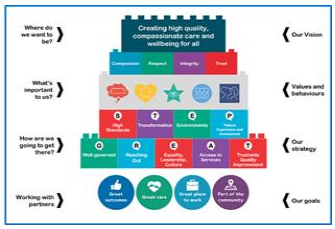


Leicestershire Partnership NHS Trust

Incident Reporting and Management Policy

This policy sets out to staff the importance of reporting incidents, how to report incidents and for responsible managers/leaders how they should manage incidents in their areas/services.

Key words: Incidents, Reporting, Learning,

Version: 5

Approved by: Safety Forum

Ratified By: Patient Safety Improvement Group (PSIG) & Incident Oversight Group

Date this version was ratified: February 2025

Date issued for publication: February 2025

Review date: September 2027

Expiry date: February 2028

Type of Policy: Clinical and non-clinical

Contents

1.0 Quick look summary 5
1.1 Version control and summary of changes 6
1.2 Key individuals involved in developing and consulting on the document 7
1.3 Governance 7
1.4 Equality Statement 7
1.5 Due Regard 7
1.6 Definitions that apply to this policy. 8
2.0 Purpose and Introduction/Why we need this policy 9
3.0 Policy Requirements 11
4.0 Duties within the Organisation 17
5.0 Consent 38
6.0 Monitoring Compliance and Effectiveness 38
7.0 References and Bibliography 40
8.0 Fraud, Bribery and Corruption consideration 41
Appendix 8 Training Needs Analysis 643
Appendix 9 The NHS Constitution 654
Appendix 10 Due Regard Screening Template 665
Appendix 11 Data Privacy Impact Assessment Screening 687

Policy On A Page

SUMMARY & AIM

What is this policy for?

Describes Trust's arrangements for reporting incidents of all types relating to patients, staff, and others of any significance and actions expected to manage and follow-up incidents.

Describe responsibilities of all staff for reporting, escalating, reviewing, investigating, and learning lessons from incidents and procedures to be followed. 'Being Open/Duty of Candour' is also considered for clinical/patient safety incidents.

To ensure LPT staff recognise importance of collation and analysis of data on incidents/near misses is an intrinsic part of patient safety as it provides valuable opportunities to learn/improve and supports the Trust in its management of risk and business priorities.

Actively encourages reporting of all types of incidents and near misses through the electronic incident reporting system 'Ulysses' and supports a 'just culture' in relation to reporting.

KEY REQUIREMENTS

What do I need to follow?

Understand your role and requirements based on your accountability and your responsibility for reporting and managing incidents.

Know why reporting incidents/near misses are important, how to do this and how to follow up on reported incidents and for managers/leaders to understand their role and responsibility in managing incidents and supporting next steps and those involved in those incidents.

All staff should feel confident, competent, and psychologically safe to report incidents using the incident reporting system 'Ulysses'.

Be aware of the types of incidents that require reporting.

To have insight of effect of incidents on patients, staff and families/next of kin.

How to escalate and communicate immediate Safety/Care issues are identified following an incident/event that signifies an unexpected level of risk / harm and/or potential for learning and improvement.

How to access training to support you in you in understanding roles/requirements around reporting and managing incidents.

Be aware of the recent and continued changes around patient safety in the NHS and where you can find additional information.

Basic information in relation incidents involving homicide, data privacy, health and safety, information technology, infection prevention and control.

TARGET AUDIENCE:

Who is involved with this policy?

Applies to all staff employed within the Trust (permanent, temporary, and honorary), students and volunteers, contractors and employees of other organisations working on the Trust's premises.

TRAINING

What training is there for this policy?

All new staff to LPT, include temporary, should receive local demonstration of how to report an incident as part of their induction.

Training is available for 'Reporting and Managing Incidents' through Ulearn & offers insight into incident reporting in the NHS, importance and value of reporting incidents, introduction to Ulysses & managing incidents well for the purpose of learning.

1.0 Quick look summary

This Policy describes the management of all incidents, clinical and non-clinical. It outlines the responsibilities of all staff for reporting, escalating, reviewing, and investigating, and identifying learning from incidents and the procedures to be followed. 'Being Open/Duty of Candour' is also considered for clinical/ patient safety incidents.

This policy applies to all staff employed within the Trust (permanent, temporary, and honorary), students and volunteers, contractors and employees of other organisations working on the Trust's premises or those where our business is conducted.

Where an incident originates from outside of Leicestershire Partnership NHS Trust (LPT), known as the Trust, it will be the responsibility of the directorates to raise concern(s) through 'Transferring Care Safely/Service Concerns' and share with the originating organisation.

If the harm is moderate or above the Corporate Patient Safety Team (CPST) will share and inform the organisation's patient safety team to which the incident belongs.

The key requirements of this policy are:

- All incidents and near misses are reported in line with timescales set out in local and corporate supporting policy/procedures.
- Immediate action is taken when required to mitigate or prevent further harm.
- To reflect the value of fair treatment of staff that supports a just culture of fairness, openness and learning in LPT by making staff feel confident to speak up, rather than fearing blame.
- Supporting staff to be open about errors, or potential errors, to identify learning and the opportunity to put safety improvement actions in place so the same errors can be prevented from being repeated.
- Consideration is given to quarantining any devices, equipment (to include disposables) or medicines associated with an incident.
- We investigate and learn from deaths as per the 'Learning from Deaths' policy.
- Safety improvement actions are taken to ensure 'we are always open with our patients and families and fully comply with the statutory 'Duty of Candour' where required, in line with the Trust's 'Culture of Candour' 'Being Open and Duty of Candour' policy.
- That prompt review, investigation and intervention is undertaken to avoid recurrence.
- Feedback to staff and patients/families is provided and the learning identified are shared/actions required are monitored and implemented.

- Patients, staff, and contractors who have been involved in an incident and as a result are 'harmed' receive appropriate support, explanation, and meaningful apology.
- Any event recognised as an incident retrospectively needing further escalation for review (in Learning from Deaths (LFD) meetings, patient feedback (complaints) or by other mechanism) is reported as described in this policy by the member of staff notified and is subjected to appropriate investigation.
- There is timely review of harm, investigation, and closure of incidents on the Ulysses system in line with agreed timescales.
- Expectation of staff in and out of hours in responding to, and, escalating when immediate Safety/Care issues are identified following an incident/event that signifies an unexpected level of risk / harm and/or potential for learning and improvement.
- Analysis of themes and trends take place, actions are agreed, monitored, and implemented.

1.1 Version control and summary of changes

Version number	Date	Comments (description change and amendments)
1	June 2021 - January 2022	New revised policy – changes in language, job titles, additional policy review, additional requests re incident type. Policy consultation Dec 2021 -2022 via email as part of trust policy sign off group.
2	Nov 2023 – Sept 2024	Complete Review & Revised in line with Patient Safety Incident Response Framework (PSIRF).
3	Nov 2024	Review and amendments from IOG group feedback, additions to reporting/escalation in line with PSIRF policy.
4	Dec 2024	Final review and alignment to PSIRF Policy updated with Homicide information, escalation of immediate Safety/Care issues are identified following an incident/event that signifies an unexpected level of risk / harm.
5	Dec 2024 - Jan 2025	Post Policy Expert Group, minor amends, addition of Clinical Support officers to 'experts'. Addition of paragraph related to patient support post incident Page22.

For Further Information Contact:

Trust Lead – Head of Patient Safety/Patient Safety Specialist

Leicestershire Partnership NHS Trust, Pen Lloyd Building - Room100, County Hall Glenfield, Leicester. LE3 8TH

1.2 Key individuals involved in developing and consulting on the review of this document:

Sue Arnold	Patient Safety Lead Nurse - CPST
Tracy Ward	Head of Patient Safety/Patient Safety Specialist
Jo Nicholls	Incident Investigation corporate lead/ Patient Safety Specialist
David Adamson	Incidents Administration Support - CPST

Incident Oversight Group (IOG) Members as of November 2023 and June 2024

Patient Safety Improvement Group (PSIG) Members as of October 2024

Trust Policy Experts

1.3 Governance

Level 2 or 3 approving delivery group – Safety Forum

Level 1 Committee to ratify policy – Incident Oversight Group and Patient Safety Improvement Group

1.4 Equality Statement

Leicestershire Partnership NHS Trust (LPT) aims to design and implement policy documents that meet the diverse needs of our service, population, and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the provisions of the Equality Act 2010 (Amendment) Regulations 2023 and promotes equal opportunities for all. This document has been assessed to ensure that no one 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.

If you would like a copy of this document in any other format, please contact lpt.corporateaffairs@nhs.net

1.5 Due Regard

LPT will ensure that due regard for equality is taken and as such will undertake an analysis of equality (assessment of impact) on existing and new policies in line with the Equality Act 2010. This process will help to ensure that:

- Strategies, policies and procedures and services are free from discrimination.
- LPT complies with current equality legislation.

- Due regard is given to equality in decision making and subsequent processes.
- Opportunities for promoting equality are identified.

Please refer to due regard assessment (Appendix 10) of this policy

1.6 Definitions that apply to this policy.

Consent: a patient's agreement for a health professional to provide care. Patients may indicate consent non-verbally (for example by presenting their arm for their pulse to be taken), orally, or in writing. For the consent to be valid, the patient must:

- be competent to take the particular decision.
- have received sufficient information to take it and not be acting under duress.

Due Regard: Having due regard for advancing equality involves:

- Removing or minimising disadvantages suffered by people due to their protected characteristics.
- Taking steps to meet the needs of people from protected groups where these are different from the needs of other people. Encouraging people from protected groups to participate in public life or in other activities where their participation is disproportionately low.

Key Abbreviations that are used and apply to this policy.

CDOP	Child Death Overview Panel
CPST	Corporate Patient Safety Team.
CQC	Care Quality Commission.
DOH	Department of Health.
DOLs	Deprivation of Liberty Safeguards.
EHA	Environmental Health Agency.
e-IRF	Electronic Incident Reporting Form.
HSE	Health and Safety Executive.
ICB's/Collaboratives	Integrated Care Boards /Commissioning collaboratives.
IG	Information Governance.
IOG	Incident Oversight Group
IRLM	Incident Review & Learning Meeting.
LFD	Learning From Deaths
LFPSE	Learn from patient safety events.
LRSAB	Leicestershire and Rutland Safeguarding Adults Board.
LRSCP	Leicestershire and Rutland Safeguarding Children Partnership.

MHRA	Medicines and Healthcare Products Regulatory Agency.
NHS	National Health Service
NHSE	National Health Service - England
PSIs	Patient Safety Incidents
PSII	Patient Safety Incident requiring investigation.
PSIG	Patient Safety Improvement Group.
PSIRF	Patient Safety Incident response Framework.
PSIRP	Patient Safety Incident Response Plan.
RIDDOR	The Reporting of Injuries, Disease, and Dangerous Occurrences Regulations.
Section 42 Enquiry	Relates to Care Act 2014, Local Authority duty to make enquiries, or have others do so, if an adult may be at risk of abuse or neglect.

2.0 Purpose and Introduction/Why we need this policy.

Recent changes and Background

In November 2023 The Trust transferred its investigation/review of incidents to align with the Patient Safety Incident Response Framework (PSIRF).

PSIRF sets out the NHS's approach to developing and maintaining effective systems and processes for responding to patient safety incidents for the purpose of learning and improving patient safety.

PSIRF replaces the Serious Incident Framework (SIF) (2015) and makes no distinction between 'Patient Safety Incidents' and 'Serious Incidents'. As such it removes the 'Serious Incidents' classification and the threshold for it. Instead, the PSIRF promotes a proportionate approach to responding to patient safety incidents by ensuring resources allocated to learning are balanced with those needed to deliver improvement.

PSIRF is not a different way of describing what came before – it fundamentally shifts how the NHS responds to patient safety incidents for learning and improvement. Unlike the SIF, the PSIRF is not an investigation framework that prescribes what to investigate. Instead, it:

- Advocates a co-ordinated and data-driven approach to patient safety incident response that prioritises compassionate engagement with those affected by patient safety incidents.
- Embeds patient safety incident response within a wider system of improvement and prompts a significant cultural shift towards systematic patient safety management.

The PSIRF supports the development and maintenance of an effective patient safety incident response system that integrates four key principles:

1) Compassionate engagement and involvement of those affected by patient safety incidents.
2) Application of a range of system-based approaches to learning from patient safety incidents.
3) Considered and proportionate responses to patient safety incidents.
4) Supportive oversight focused on strengthening response system functioning and improvement.

The Trusts approach and methodologies to be used for investigation/review of incidents is detailed in the Patient Safety Incident Response Plan (PSIRP) and can assessed via the StaffNet and public website. This document details both the national priorities / expectations and locally agreed investigation approaches based on safety priorities and the ability to learn and improve from patient safety incidents.

Notification of Incidents in LPT and the influence of PSIRF

The Trust is committed to supporting and embedding a positive reporting and learning culture to enable the organisation to respond and learn where patient/staff outcomes are not as expected or a 'near miss' has been reported through the electronic incident reporting system 'Ulysses' and supports a 'just culture' in relation to such reporting.
This policy has been reviewed in line with PSIRF and describes the Trust's arrangements for the reporting and management of all incidents, clinical and non-clinical involving staff, patients, and others and of any significance and the actions expected to manage and follow-up such incidents. It also ensures that arrangements are in place to adhere to legislative and reporting requirements for NHS England's 'Learning from Patient safety Events (LFPSE)' in line with the Patient Safety Strategy (2019), Health and Safety Executive (HSE), Care Quality Commission (CQC) registration process, the Trusts integrated care boards and collaboratives and both internal and external stakeholders.

We strive to support our patients first, and foremost, every time when their care may have not gone as expected; this policy follows the guidance NHS England Patient Safety Strategy (2019). The focus on reporting all incidents should be on analysing the contributory factors, including human factors with the purpose of learning and safety/improvement actions put in place where required. This is undertaken on a background of 'openness' and 'transparency', supporting patients, family, and staff through the process.

All staff should feel confident, competent, and psychologically safe to report incidents and where staff do not feel able, they should discuss with a trusted leader and where this is not possible or does not result in action expected there is an option to raise concerns through 'Freedom to Speak up Guardians' (FTSU); staff are actively

encouraged to discuss with the CPST if they consider they have not been heard by local/trusted leaders prior to raising concerns with FTSU.

The policy applies to all staff employed within the Trust (permanent, temporary, and honorary), students and volunteers, contractors and employees of other organisations working on the Trust's premises, or on other premises where services are provided by LPT, or which occur as a direct consequence of LPT care.

3.0 Policy Requirements

This policy aims to establish a clear and consistent approach to the reporting, investigation/reviewing, and management of incidents, including near misses so that LPT provides a safe environment for patients, staff, visitors, and contractors. In particular:

- Sets out the basic requirements for reporting an incident via Ulysses reporting system that generates electronic incident report form, known as a eIRF.
- Ensure a 'Just Culture' is promoted, and embedded so that staff are assured that the Trust will have an open and just environment and that it is the Trust Policy to do so.
- Ensure all incidents are managed in a timely, effective, and organised manner.
- Ensure robust record keeping and reporting mechanisms are in place.
- Ensure clear lines of accountability and responsibility are identified for all elements of incident reporting and the management of these incidents.
- Ensure that all relevant staff, including bank, locum and agency staff are aware of the communication systems in place for the reporting and management of all types of incidents, via induction and training.
- Establish key communication mechanisms with patients, family and/or carers in line with the 'Culture of Candour 'Duty of candour/Being Open' Policy.
- Ensure all appropriate levels of debrief and support to staff and the sharing of learning identified takes place following incidents. **See Appendix 1** for guidance for staff using 'Debrief Flow Chart' following an incident for staff members and **Appendix 2** the 'Provision of Staff Welfare and Support Debrief Tool'. The Post-Incident Pathway for Staff Support (PIPSS) Policy (2024) also gives additional detail of staff support describing the support available to staff following a Traumatic Incident, including incidents of violence and aggression.
- Ensure all relevant internal and external Stakeholders, Agencies, and Regulatory bodies are engaged, involved, and informed in line with National policy and guidance.
- Ensure any learning identified from reported incidents, is recorded, and shared with those involved and managers/leaders take appropriate action to avoid a recurrence, including, where required, making changes to system, process, practice and/or the environment to improve patient and staff safety.

It is important to provide assurance to staff that no disciplinary action will result from reporting an incident (including errors and near misses), unless there is evidence of:

- Criminal or malicious activity.
- Professional malpractice and lack of insight.
- Acts of gross misconduct.
- Errors, mistakes, or violations have not been reported.

Under the above circumstances, Human Resource (HR) policies will be followed which may include referral/reporting to professional bodies being considered and is outside of the incident reporting process.

The responsibilities of all staff for reporting, investigating, and learning lessons from patient safety investigations(PSIs) and patient safety reviews (PSRs) are set out in this policy together with the Trust's Patient Safety Incident response plan (PSIRP); this describes the Trusts plans for Patient Safety Incident learning Responses.

Confidentiality application to Incident Reporting

Full names should only be recorded in the required section of the eIRF, not in the narrative/incident description. Within investigation/review reports undertaken relating to an incident staff should be referred to by their job title where practical and other individuals should be referred to by initials only or by details following permission granted and recorded from patient/family.

Definition of an incident

An incident is an adverse event that gives rise to, or has the potential to produce, unexpected or unwanted effects which could be detrimental to the safety or health of and can include the following:

- Patients
- Staff
- Contractors
- Members of the public
- Organisation
- Property
- Equipment

The Trust encourages the reporting of all incidents both patient and non-patient. This includes:

- Incidents that you have been involved in
- Incidents that you may have witnessed.
- Incidents that caused no harm or minimal harm
- Incidents with a more serious outcome
- Prevented patient safety incidents also known as 'near misses'.

Definition of a Near Miss

A near miss is an incident that was prevented by chance rather than part of the process. An example of a prevented patient safety incident:

- Medication was about to be administered to a patient when it was realised that it was the wrong patient.

Definitions associated with Incident Reporting

Hazard

Any object, location or set of circumstances that pose a risk and have the potential to cause harm, loss, or damage i.e., a bed left on a corridor, which could block a fire escape or cause someone to trip or fall; unlabelled syringes placed in a tray, which could be used inappropriately creating the opportunity for error.

Risk

The probability that a specific adverse event will occur in a specific time, or, because of a specific situation (hazard) i.e.,

- Medication can be a hazard; the risk is the probability of the hazardous outcome being realised. When there is such an outcome this would be an incident that requires reporting. Where there is a mistake or an error involving a medication but there is no harm this is still an incident that requires reporting. If a mistake or error was intercepted so that it did not actually happen this would be a reportable ‘near-miss’ from which learning is likely to be identified.

Specific information related to ‘Incidents’, their type and local/national responses required.

Definition of these specific Incidents

Any unexpected or unintended event, which could have or did lead to harm, loss, or damage, for example:

- Equipment malfunction,
- Breach of confidentiality,
- Wrong dose of medication administered,
- Verbal abuse by patient/visitor or member of staff,
- Physical injury.

In addition, all ‘Never Events’ as defined by NHS England (2018) are incidents reportable as patient safety incident and require investigation under the current patient safety incident investigation (PSII)’s outlined in the Trust’s Patient Safety Incident Response Plan (PSIRP).

RIDDOR reportable Incident - see Appendix 5 for further information.

Any incident or occurrence defined within the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR), e.g.

- Deaths
- Specified Injuries
- Injuries lasting more than 7 days (where an employee or self-employed person has an accident, and the person is away from work or unable to work normally for more than seven days).
- Injuries to members of the public where they are taken to hospital.
- Work related diseases/exposure to hazardous substances and dangerous occurrences.
- There are also injuries to patients that become reportable; services are to be guided by the Health & Safety Team.

Incidents that are associated with 'Safeguarding Children and Adults'

Local Authorities have a particular role to play in safeguarding adults and children and young people in vulnerable circumstances. Providers and integrated care boards (ICBs)/specialist commissioners must ensure that information about abuse or potential abuse is shared with Local Authority (LA) safeguarding teams.

Providers and ICBs commissioners must liaise regularly with the LA safeguarding lead(s) to ensure that there is a coherent multi-agency approach to investigating safeguarding concerns, which is agreed by relevant partners.

- There may be occasions whereby Safeguarding Section 42 enquiry (allegation of, or is at risk of, abuse/neglect) investigations are linked to patient safety investigations: services will be guided by the CPST and Safeguarding Teams.

Child deaths (all subject to Child Death Overview Panel (CDOP)), harm and serious sexual abuse are likely to trigger a patient safety review of some level; however, all are reported to the Leicestershire and Rutland Safeguarding Children Partnership (LRSCP) and the plan for LPT investigation discussed and recorded with the LRSCP.

The interface between and local safeguarding procedures are articulated in the local multi-agency safeguarding protocol and policies and is further detailed in LPTs PSIRP plan.

Further information re - Safeguarding Children and Child harm incidents

Where a child has been significantly harmed but not died because of an incident, the following considerations need to be explored as to whether the incident meets the threshold of a PSII or not:

- Has the harm occurred on NHS premises, whilst in receipt of NHS funded care, or caused by the direct actions of healthcare staff?

If no to all the above, it is useful to consider whether the child has been in receipt of healthcare within the last 12 months. If so, the case will need to be reviewed under the Trusts PSII framework related to the local PSIRP as well as to the LRSCP.

Any child under the age of 16 admitted to an adult mental health ward must be notified to Safeguarding for Children, reported on Ulysses and will require a PSII and the CQC notified.

Safeguarding Adults

A vulnerable adult is someone over the age of 18 years in need of services by reason of mental or other disability who is unable to take care of or protect themselves against harm or exploitation. All incidents of abuse including neglect to a vulnerable adult are notified through Safeguarding Adults procedures as well as reporting as an incident on Ulysses.

Cases of death or significant harm may also be investigated as a Serious Case Review under Safeguarding Adults procedures through the Leicestershire and Rutland Safeguarding Adults Board (LRSAB). The interagency decision to investigate as a Safeguarding Adult Review (SAR) should not delay the investigation as an PSII. The completed PSII report will form the basis of any SAR individual management report (IMR).

Incidents linked to known complications/risk associated with delivery of care.

An adverse outcome reasonably associated with NHS activity; a known complication of that treatment/therapy (such as an operation/procedure/medication) is not an incident; however, it does gives give a service an opportunity to review patient care, the interventions and should be considered for learning. Where death has occurred, such outcomes should be subject to Morbidity and Mortality Meeting review/Modified Structured Judgement Case Review (mSJCR) in the case of deaths (see 'Learning from Deaths' Policy).

Incidents identified after the event .

Directorates must ensure that an incident/event involving a patient recognised later and requires reporting as an incident and likely requiring a potential higher level of investigation, including PSII (in Mortality and Morbidity meetings or by other mechanism, i.e., notified by family or 3rd party) is reported and is subjected to appropriate review through the usual Trust processes and the CPST notified.

Notifications to Care Quality Commission (CQC) of incidents involving patients/service users required under 'Guidance and Regulation' by CQC (Regulation 18(2), Care Quality Commission (Registration) Regulations 2009).

https://www.cqc.org.uk/guidance-regulation/providers/notifications (relates to the new 2024 standards for regulation)

The following incidents must be reported using the relevant CQC approach online/by email of bespoke documents:

- **Allegations of abuse (safeguarding)**via LFPSE
- **Children and young people in adult psychiatric units**
- **Death of a detained mental health patient (or liable to be detained)** via LFPSE **and** online notification form or email completed word form including the LFPSE.
- **Death of a person using a service at LPT** where the person died while a regulated activity was being provided or their death may have been a result of the regulated activity or how it was provided via LFPSE.
- **Events that stop a service running safely and properly** (you cannot meet people's assessed needs safely, for example, due to staff absence or damage to premises, or a utility, fire alarm, call systems or other safety equipment fails for more than 24 hours) via LFPSE.
- **Outcome of an application to deprive a person of their liberty (DoLS):** As soon as LPT is notified of the outcome of an application to deprive a person of their liberty, you must tell us:

➢ about the outcome of the application to deprive a person of their liberty
➢ about the outcome of any application made to the Court of Protection. Do this even where you have not made the application yourself. For example, the local authority may have applied to the court.

➢ if an application is withdrawn.

- **Police involvement in an incident in a service that is reported to, or to be investigated by the police.** (**NHS trusts** do not need to notify us about **police attendance**). We must notify CQC of incidents which may affect someone's health, safety and welfare when using, visiting, or working at your service; this may be by notification of death, serious injury and abuse and therefore separate notification regarding police involvement is **NOT** required. Notification of Police involvement is via online or email copy of completed word document.
- **Serious injury to a person using services** that includes the person was seriously injured while a regulated activity was being provided or their injury may have been a result of the regulated activity or how it was provided. If the serious injury is the result of an assault, allegation of abuse notification form is to be used instead.
- **Unauthorised absence**: Only services with a specific security designation of low, medium, or high security need to tell us about:

➢ an unauthorised absence of a person detained (or liable to be detained) under the Mental Health Act 1983.
➢ when someone returns from an unauthorised absence.

All the above must be undertaken either by notification via CQC portal or by completion of word document. Notifications are undertaken in conjunction with

the Head of Nursing for the appropriate individual directorates and the Quality & Compliance Team. Reference must always be made to the incident/LFPSE details and a copy where possible attached to the incident; if this is not possible the incident must be updated with this notification details.

4.0 Duties within the Organisation - Roles and Responsibilities

Whole Trust

LPT has an obligation to patients who use our services and to provide staff with a mechanism to report staff/organisational incidents and on many levels a legal obligation to ensure that all incidents, accidents and near misses are managed, reported, and actioned appropriately. We are accountable to our ICBs/specialist commissioners, through contracting and commissioning arrangements, NHS England (NHSE), CQC and Information Commissioners Office (ICO), Public Health England (PHE) and Health and Safety Executive (HSE). This list is not exhaustive.

The Trust recognises its role and responsibility to external regulatory and monitoring agencies, and other external stakeholders. Overview of External Stakeholders who may influence/request incident investigation information and responses at LPT are described in greater detail on Page 26 of policy.

Chief Executive has:

- Overall responsibility for the implementation of this policy.

Trust Board of Directors will:

- Receive learning reports related to Trust incident reporting on a bi-monthly basis.
- Consider any independent investigation reports conducted.
- Commit to the requirement to follow the Duty of candour/ Being Open requirements as determined by Regulation Standard 20 of CQC.

The Quality and Safety Forum (Q&S) Forum will:

- Consider patient safety reports on incident management and learning.

Executive Director of Nursing, Allied Health professionals & Quality will:

- Ensure that this policy is implemented through robust systems and processes and that there are effective reporting and monitoring processes in place.

Medical Director will:

- Ensure that all medical staff are fully aware of this policy to ensure they adhere to its requirements; including junior doctors as part of induction so they are confident and able to report incidents and near-misses.

- As Caldicott Guardian, ensure that effective systems are in place to maintain the security of identifiable data.

All Directors will within their own areas of responsibility

- Ensure that internal and external reporting requirements are met.
- Ensure all incidents are investigated appropriately according to the severity of the incident.
- Ensure that effective analysis and learning systems are in place within their service(s) and that assurance and monitoring takes place.
- Ensure that their service(s) complies with and follows 'Duty of Candour/Being Open' with all those affected by an incident, together with effective support mechanisms for staff.
- Consider incident and aggregated data in the identification of risks and address risks through risk reduction measures and to improve quality of services.
- Ensure that staff attend any training required to comply with the requirements of this policy according to the training needs analysis.
- Adhere to policies of commissioning organisations, taking responsibility for producing reports that meet the required timescale and to report to the Trust Board of Directors on patient safety investigation findings and learning.

CPST will ensure that:

- Incidents are reported, monitored, and managed in line with this policy.
- Where there is scope for Trust wide learning; effective dissemination takes place.
- Trends and areas for improvement are identified and shared with directorates via Trust Committees, education and training programmes, intranet webpages, newsletters and bulletins and support given as requested to undertake this at local directorate level.
- In conjunction, and, when requested by the Directorate Clinical Quality Governance Teams; ensure information and training is provided for staff regarding reporting, appropriate harm level reporting and investigation of incidents and completion of e-IRFs.
- Additional support will be provided for the clinical leadership teams to ensure triage of incidents is timely by an electronic email generated daily triage report and support with escalation of incidents is undertaken as required.
- Weekly sharing to all directorates named individuals of incidents that remain outstanding for closure beyond 15 working days; this will also facilitate monthly/bi-monthly position to Executive Team.
- Incidents that are 'saved for later'(started but not completed by reporter) and those with patient (PID) or staff (SID) identifiable information

contained in the body of the incident will be returned to the reporter for action. A monthly report will be collated and shared collectively with each governance team for action. Enabling Directorate will be reviewed/escalated by CPST to respective dept. managers.

Heads of Service/Service Managers/Heads of Nursing will:

- Have systems and processes in place to deliver on the required duties of directors as listed above.
- Ensure that all staff within their area are aware of, and of and understand this policy.
- Ensure that all incidents are reported and investigated proportionate to the severity of the incident.
- Ensure that patients/families/carers are informed and kept updated of incident providing timely feedback that is recorded in the electronic incident record.

Directorate Clinical Quality Governance Teams

- In liaison with the CPST provide quality assurance of the reporting and the appropriate recording of harm related to incidents with managers where there are issues of concern, offering support and re-training as required.
- Produce monthly (and at other requested intervals) incident reports (to include themes and trends), including 'Being open/Duty of candour' compliance and submission to Patient Safety Improvement Group (PSIG) and Incident Oversight Group (IOG).
- Work with and support the local teams and the CPST to ensure the timely management of incidents, providing incident information as required.
- Work in liaison with their Directorate Teams and the CPST as required to support /arrange training to staff on all aspects of incident management.
- Work in liaison with the CPST to ensure that all records that relate to an incident or investigation are stored within Ulysses to ensure there is a central repository of all relevant information. This includes investigation records & meeting/interview notes, learning (boards) and communication with external stakeholders. (NB in very extreme cases of sensitivity, a file note must be made on Ulysses to indicate the existence and location of the information).
- To support the Trust to meet its external reporting responsibilities by liaising with the various leads and complying with requests for information from CPST.
- To support and enable all staff with leadership and management responsibility for incident management to undertake their duties in line with good incident management.
- To support the completion of saved for later and PIS/SID info reports for correction/completion as shared by CPST.

Specialist staff

- Advise and assist in the reporting, investigation, and the timely action of incidents relevant to their role.
- Specialist staff can include Health and Safety Advisors, members of CPST, Manual Handling Lead, Infection Prevention & Control Lead, Safeguarding Lead, Trust Fire Officer, Pharmacy, Trust Security Management Advisor, Emergency Planning Lead, Estates Managers, Clinical Safety Officers (CSO's) etc.

All staff with Leadership and Management Responsibility will:

- Ensure that they, and the staff they are responsible for comply with and support the implementation of this policy.
- Ensure staff report all incidents effectively and where necessary, local investigations are undertaken, learning identified and implemented and that patients/families are kept informed.
- Escalate concerns and incidents that may meet the threshold for a further level of review and/or investigation.
- Ensure all incidents are correctly categorised, the level of harm is accurate and appropriate action has been taken to both ensure the patient and/or member of staff is safe and escalate/act as part of the closure of all incidents. It is a requirement that this information is recorded on Ulysses.
- Ensure they feedback to staff who have reported incidents and to consider how they will share the wider knowledge of reported incidents/learning with their teams and take action to mitigate against recurrence; this must form part of their incident closure evidence.
- Ensure that all staff can access training in the form of local induction covering incident reporting and support additional training in relation to incident management, investigation and learning according to their roles.
- Consider and use incident data in risk assessments as appropriate as part of complying with the Risk Register process in conjunction with their local clinical governance teams.
- Ensure that incidents are investigated and closed in a timely way; this should be within 15 working days of most incidents being reported **(except for incidents that are awaiting initial review and may lead to a PSI review)** and the level of reported harm of all incidents and approve/amend them before closure submission in Ulysses.
- Undertake, participate themselves and ensure staff participation in any local incident investigation.
- Are responsible for supporting staff involved in and/or affected by an incident. See **Appendix 1** for guidance for staff using 'Debrief Flow Chart' following an incident for staff members and **Appendix 2** the 'Provision of Staff Welfare and

Support Debrief Tool'. Further information can be found in 'The Post-Incident Pathway for Staff Support (PIPSS) Policy' (2024) which also gives additional detail of support available to staff following a Traumatic Incident, including incidents of violence and aggression.

- Ensure that learning identified from incidents are fed into local forums and that they review trends on a regular basis in conjunction with line manager and clinical governance teams and where necessary, develop safety and quality improvement plans to reduce recurrence.
- Ensure a regular reporting mechanism exists with line manager, Matron, Deputy Heads of Nursing or Head of Service/Nursing as appropriate.

Summary - All teams/employees as individuals

- Those involved in managing incidents must ensure they are appropriately categorised, harm levels accurately recorded, and all records related to incidents are stored only in Ulysses. No local electronic files related to incidents will be kept.
- Currently, Health & Safety/RIDDOR information is stored on other files and provide the information as requested.
- Attend/undertake the required local training relevant to this policy at local induction.
- Read and comply with the content of this policy.
- Report all incidents and near-misses that they are involved in or witness/discover and act on and report in accordance with this policy any incident that is brought to their attention by a patient, family member, visitor or contractor and colleague.
- Comply with the requirements of 'Being Open Policy/Culture of candour' in relation to incidents in communicating incident information to those affected and undertake a meaningful apology and always say 'sorry'.
- Participate in investigation and implementation of learning from incidents.
- Not to discuss via social media or communicate directly with the media relating to incidents and should direct all enquiries from the media to the Trust Communication Lead or the Chief Executive's office.

Quality checking of Incidents reported.

All staff who access the e-IRF record have the responsibility to quality check the recorded details to ensure all relevant fields are completed and in line with the incident description, learning identified has been recorded and that there is no patient/staff identifiable information within the main incident description to avoid information governance breaches (other designated places exist for this information in the individual incident report).

If, during the final approval process, issues are identified the incident will be reviewed and moved back into 'awaiting review' by the manager for the area. Support and facilitation will be undertaken by the CPST (incidents) and

communication will be sent via Ulysses communication section to explain the reasons why the incident cannot be approved and should be returned to the reporter.

It is also recommended at this point that all information related to equality and diversity should be completed by using the drop-down section in the area of patient/staff involved and be completed with the current information available.

Reporting to the Learning from Patient Safety Events (LFPSE's)

(LFPSE service is a national NHS system for the recording and analysis of patient safety events that occur in healthcare. The service introduces a range of innovations to support the NHS to improve learning from the over 2.5 million patient safety events recorded each year, to help make care safer. Here at LPT all Patient Safety Incidents (PSI) are automatically uploaded onto the national database LFPSE immediately the incident forms are completed. More information about this service can be found here. https://www.england.nhs.uk/patient-safety/patient-safety-insight/learning-from-patient-safety-events/learn-from-patient-safety-events-service/

Part of this new process is that our Commissioners and regulators have access to review these incidents and may ask questions/clarification about our processes for learning.

Incident Reporting Process - Immediate Action Following an Incident.

Identifying an incident or near miss is the first stage of risk management. Any member(s) of staff present when an incident is identified must take immediate action to reduce further risk and in maintaining safety, ensure that their own safety is not compromised and that of the patient(s) or others.

Once the immediate situation has been addressed, it is the responsibility of all members of staff to bring an incident or near miss to the attention of the most senior member of staff on duty/on call in the designated area.

The following factors should be considered to determine the necessary escalation:

- The extent of harm caused and the immediate first aid and support needed to injured or traumatised persons.
- The adequacy of the immediate nursing, medical and management response, and the need for specialist advice/support
- The safety of the situation and the potential for further harm.
- The need to inform the patient(s) and or their family/representative. Any patient, those involved, including staff, in the incident should be supported and informed of what appears to have happened, its consequences as far as is known and treatment available and what immediate actions are necessary to minimise further risk or injury. This communication should take place as soon as possible and an apology given.

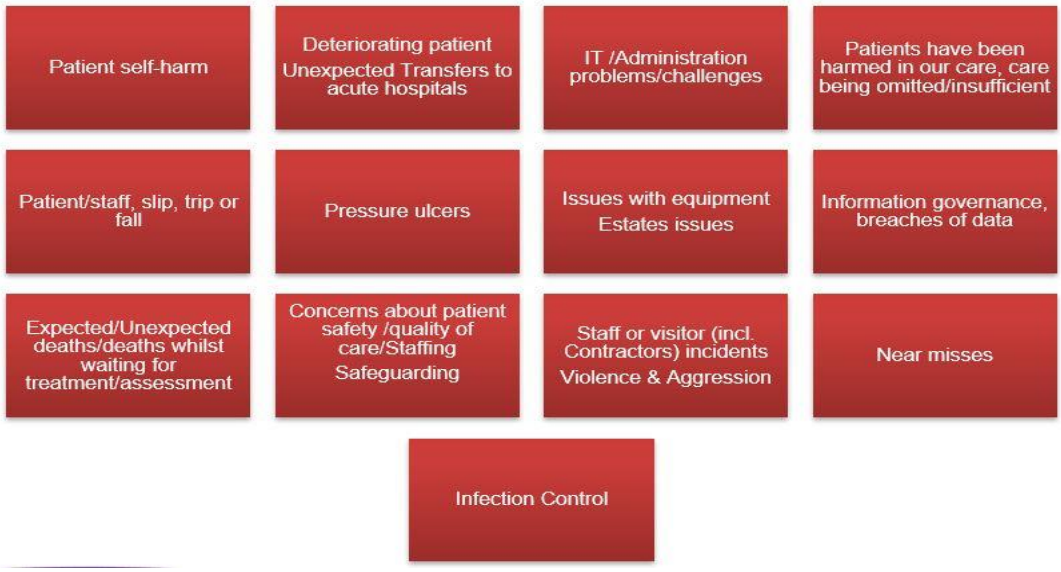
- The need to support service users, staff and others affected by the incident.
- The Registered Nurse (RN), Nurse Associate, Support Worker/AHP/Doctor attending or identifying a patient related incident is responsible for recording the incident details in the patient's records, before they end their shift/move onto the next visit/clinic in case of the community. **It is not acceptable to delegate or carry over this responsibility.**
- Nurse Associate/Support Workers who identify incidents must escalate what appears to have happened to their line manager. It is the responsibility of the line manager to whom the incident has been escalated to review plans of care, acknowledging, and updating risk assessments as required. **It is not acceptable to delegate or carry over this responsibility.**
- RNs / AHP's in charge of shifts/Teams/Mental Health Clinical Duty Managers, On-Call Managers should also include updating local handover documents with basic incident information and immediate actions taken. This must include any escalation undertaken or advised to do by a more senior clinician. **It is not acceptable to delegate or carry over this responsibility.**
- Currently, Band 6 and above RNs / AHP's /Mental Health Clinical Duty Managers are responsible for updating the initial incident report regarding the outcome (known as 'managers sign off'); i.e., patient transferred to acute hospital following a fall for x-ray and returns to ward during the shift incident occurred.

Completion of incident forms

Incidents should be reported within 24 hours, or, as close to the time of the incident as practicably possible of staff becoming aware of the event and ideally as soon as possible after initial management of the incident. This includes all types of incidents. All sections of the form should be completed covering immediate post-incident actions and is accessed via the Trusts intranet page or by staff accessing Ulysses through local secure electronic access as per favourites or Ulysses icon on desktops/laptop.

When an incident is recognised, or the Trust is notified sometime after the event the responsible directorate member of staff who is notified must report the incident as described in this policy. **The passage of time is not a reason not to report.**

Tips - Below are some examples of what type of incidents to report – further examples of commonly reported incidents can be found in Appendix 4.



Things to consider when reporting:

- To support the identification and sharing of incident trends and themes the reporter is required to allocate the incident a cause groups/types (also known as a category and sub-category), staff will be able to find one that resembles or is close to one they are wanting to report.
- The reporter is usually the person who witnessed the incident, they are in a unique position in understanding the events.
- Personal demographics must not be included in the body of the report.
- The incident report should be free from jargon, opinion and be factually accurate.
- The use of situation, background, assessment, review (SBAR) methodology allows for a good structure for reporting and is actively encouraged.

Immediate Management of the Incident and communications

- The senior member of staff in charge of the area where the incident occurred should be informed immediately. It is their responsibility to ensure that the incident has been dealt with and any necessary further reporting of the incident takes place. This includes ensuring, that where necessary, the next of kin/family have been contacted and an incident form correctly completed so that reporting to Senior Staff/Directors can take place if appropriate; this is known as ‘Heads Up’ when it is submitted via Ulysses and is automatically generated in relation to certain types of incidents.
- The manager of the area also has a responsibility of understanding the level of harm to patient(s)/staff and that others are safe.
- Staff involved must ensure that the patient receives appropriate care and intervention according to the incident and that the patient is kept informed.

Staff should consider if the patient would benefit from a supportive conversation around how they are feeling about what has happened, what next steps are and, for example, in instances of patient self-harm, the patient is given an opportunity to discuss/reflect what led to the incident and what support staff can put in place.

- The most senior member of staff has the responsibility of verbally reporting incidents that have the potential to be a potential PSIs that may require further escalation and review.

Supporting staff and those involved

The manager of the area will ensure that those involved in/affected by incidents are supported following an incident. The Trust values its staff and recognises that they are its most valuable resource. In support of this principle, all staff members involved or affected by a traumatic or stressful incident should be offered support from their line manager immediately or as soon as practically possible. The appropriate manager will need to assess the needs of the staff involved and where necessary implement a plan to assist in their recovery from any harmful or stress related reactions. The Debrief Pathway is included in the appendices of this policy and the Post-Incident Pathway for Staff Support (PIPSS) Policy (2024) also gives additional detail of staff support describing the support available to staff following a Traumatic Incident, including incidents of violence and aggression. This can be found on the staff intranet.

Where an incident of violence and aggression leading to assault/injury to a member of staff has been reported, an alert is automatically sent as a notification to the Trust Security Management Advisor via Ulysses.

Immediate Safety/Care issues identified following an incident that signifies an unexpected level of risk / harm and/or potential for learning and improvement.

Where a patient safety event is reported that signifies an unexpected level of risk / harm and/or potential for learning and improvement an MDT Review meeting will be arranged, chaired by the Director of Nursing or designated deputy or the Trust Medical Director or designated deputy, where the incident will be reviewed, and proportionate learning response agreed, and an initial learning response lead allocated. All discussion and decisions will be recorded on Ulysses. This is likely to occur before IRLM, however, the patient safety incident initial findings will go on to be presented at the next available IRLM.

On some occasions the escalation in relation to immediate safety/care issues that signifies an unexpected level of risk / harm and/or potential for learning and improvement may arise following further review of a patient safety incident at the ISMR stage and also following review at IRLM and further MDT review by the Director of Nursing or designated deputy or the Trust Medical Director or designated deputy sought to agree a response and understand the risks associated with the

incident and impact on patient(s).

For further information and flow chart to support staff - See Appendix 3

Guidance for staff when: 'Immediate Safety/Care issues are identified following an incident/event that signifies an unexpected level of risk / harm and/or potential for learning and improvement'.

Management of incidents where more than one Department or Organisation is involved.

- Where an incident is discovered within a department, it is the responsibility of staff to report it in line with current LPT policy. However, if the incident may have occurred in or also involved another department, and where this is the case, you must inform your line manager who will liaise with the other department to ensure that appropriate actions are identified to reduce the likelihood of the incident recurring. CPST may also assist by coordinating an initial review.
- Where an incident is discovered which may have originated in another organisation who were involved in the care of the patient, clinical governance teams should contact the CPST so that the appropriate stakeholders can be informed and involved in the initial review and any following investigation.

External reporting and escalation of incidents

'Specialist Staff'/Line Managers/CPST should ensure that:

- Any RIDDOR incidents are notified to the Trust Health and Safety Team, if they have not identified them; they are responsible for reporting to the HSE without delay. (**See Appendix 5 for more information**).
- If a member of staff is involved, they are provided with appropriate support including a referral to Occupational Health Department or local Emergency Department if injured and where this is required.
- CPST, in conjunction with Line Managers/Deputy Heads of Nursing/Heads of Nursing/Services will ensure that any Initial Service Managers Reports (ISMR's) are requested for all incidents that may require higher level of investigation.
- Directorate Clinical Quality Governance Teams are responsible for ensuring completion and return to the CPST within the local timescale agreed and that local clinical review/oversight has taken place in readiness for review at the weekly Incident Review and Learning Meeting (IRLM) and in readiness for sharing with external bodies such as CQC and NHSE as requested.
- Under PSIRF ISMRs are shared collaboratively by CPST with ICBs/commissioners as part of IRLM not as part of their oversight prior to next steps investigation.

Incidents involving Trust Health and Safety Compliance

If the incident is identified as reportable under RIDDOR or has resulted in significant harm, injury or near miss to a member of staff, visitor, or contractor and on some occasions patient(s); results physical or criminal damage to the buildings or environment; is in breach or contravenes any health and safety legislation. **(See Appendix 5 for more information).**

Trust Health & Safety Compliance Team will be responsible for:

- Assessing the level of investigation required and providing specialist advice to the CPST and local directorate teams.
- Undertake as appropriate RIDDOR reporting and lead/contribute to incident investigation.
- To liaise with the Health & Safety Executive as required.

Recording Harm Levels

Definitions of Levels of Harm currently applied in Incident Reporting :

Near Miss: incidents that had the potential to cause harm but were prevented. Near misses are important for identifying and mitigating future risks and offers opportunity for learning and improving.
No harm: incidents where no harm resulted, but there was potential for harm. For example, drug error that did not cause any ill effects, falls with no injury, violence, or aggression not resulting in any injury or harm. Frequently similar/same 'no harm incidents' offer an opportunity for learning and improving and could be an indication that there are gaps in systems/processes that staff are working with.

Low/Minor harm: incident that required extra observation or minor treatment, not requiring intervention from an acute provider i.e., transfer to Emergency Department and caused minimal harm, to one or more persons receiving NHS-funded care.

Moderate harm: incident that resulted in the patient requiring healthcare intervention as a result i.e., transfer to Emergency Department and which caused significant but not permanent harm, additional care that delayed discharge and treatment to one or more persons receiving NHS-funded care.
Staff injury i.e., because of assault may also fall under this category.

Severe harm: incident that appears to have resulted in permanent harm (**physical or psychological**) to one or more persons receiving NHS funded care.
Catastrophic/Death: incident that directly resulted in the death of one or more persons receiving NHS-funded care.

As the NHS moves towards a more safety critical industry approach through PSIRF and the use of system and human factors approach to investigations, near miss and low harm incidents where the learning is so great can also be the focus of next step

investigations as well as the recognition that '**psychological harm**' to patients and staff cannot always be quantified by the 'actual' level of harm caused to them.

Homicide Incident Investigation and Recording in mental health.

Homicides committed by those in receipt of mental health care have devastating consequences for the family of the victim(s), patients and their families and can have a profound impact on all parties involved. Information shared with the Trust relating to homicides even if the person involved/allegedly committed the act of homicide is **no longer under the Trust's care should be reported as an incident**; a review can be undertaken as to next steps in this circumstance and decisions made in conjunction with safeguarding, senior trust mental health staff and subject specialist as required.

Similarly, where a patient who is under the care of LPT is the victim of homicide – this should be reviewed to consider if there was any opportunity to safeguard our patient.

These incidents often require complex multi-agency investigation involving internal and external stakeholders across geographical and organisational boundaries. There is a regionally led standardised approach to investigating such incidents (Single Operating Model for Investigating Mental Health Homicides within NHS England). The main purpose of which is to:

- Ensure mental health care related homicides are investigated in a way that lessons can be learned effectively to prevent recurrence.
- Consider if a wider investigation is needed into the commissioning and configuration of services that may have contributed to the homicide incident.
- Review the care and treatment and establish if the incident could have been predicted or prevented and what lessons can be learned.
- Provide additional objectivity for the family and wider public.
- Ensure any recommendations made are implemented through effective action planning and are then monitored by providers and commissioners.
- Ensure there is early consideration for joint investigations where other agencies are carrying out investigation into the same incident/s, for example in cases of the death of a child and that where possible a single investigation is commissioned and together, they agree the approach to the timing, sharing of information and confidentiality issues as well as communications with families, carers, staff, and the media.

The regional investigation team will ensure that consent to access information and to share information with the victim's family is sought at the earliest opportunity.

Homicide Review Process

This has three defined stages:

Stage 1 – Incident recording and Initial service managers Review (ISMR) completed within 72hrs of notification.

a) In the event of an incident all relevant and known details should be recorded on Ulysses as soon as staff are aware.

b) Formal notification by email of the homicide to Trust Safeguarding Lead is to be undertaken by CPST to Trust Head of Safeguarding, Deputy Director of Nursing with responsibility for Trust Safeguarding (& copying in Trust safeguarding duty generic email lpt.safeguardingduty@nhs.net) to ensure safeguarding are engaged at an early stage to initiate required safeguarding responsibilities.
c) The incident will be reviewed and recorded as such on the Trust incident reporting system.
d) CPST will inform NHSE and the relevant ICBs/specialist Commissioner incident/quality lead.
e) NHSE quality lead will alert the Regional Investigations Team and ensure with the provider that ISMR review is completed by the provider.
f) ISMR informs of the any early learning immediate actions taken, or initiated relating to:

- Providing assurance that the safety of staff, patients and the public is protected.
- Gaining Support of staff/teams involved.
- Proposing the appropriate level of investigation Homicide incidents are a national defined as a priority for PSII.
- Communicating with relevant individuals and organisations including the families of victims and perpetrators, Police, Coroner, HSE, NHSE and CQC, as required.
- The provider should actively seek the details of the victim/s and families at an early stage.

g. **(Local Action)** As the incident signifies an unexpected level of risk / harm and / or potential for learning and improvement a Multidisciplinary Team (MDT) Review meeting will be arranged, chaired by the Director of Nursing or designated deputy as soon as possible **– within 24hrs of incident notification.**

(Suggested MDT attendees, Medical Director or deputy, Head of Nursing - Directorate of Mental Health (DMH) (or deputy), DMH Clinical Director, Safeguarding Team representative, senior CPST team member).

At this meeting the incident will be reviewed, a proportionate learning response agreed, and an initial learning response lead allocated to complete the initial service managers review(ISMR). The patient safety incident initial findings will go on to be presented at the next available IRLM. All attendees, meeting discussion points and decisions/individual actions will be recorded in the specific contact/meeting section on Ulysses by CPST representative. Agreement of information to be shared with Trust Communication Manager at this stage.

At this point, named family liaison person will be identified and CPST will contact local Police through trust liaison officers and identify agreed named Police contact with regards to status of their investigation progress and ability to contact family of victim and perpetrator.

h. The CPST will inform NHS England and the relevant Commissioner incident/ quality lead.
i. It is expected that NHS England quality lead will alert the Regional Investigations Team.
j. **(Local Action)** LPT will share the completed ISMR following review and agreement by executive team with designated commissioner and NHSE named link via the CPST.
k. **(Local Action)** All correspondence (i.e., email) related to the incident will be uploaded onto Ulysses and meetings recorded in the specific contact/meeting section on Ulysses by CPST.

Stage 2 Independent review commissioned by the provider.

A PSII will be required to undertaken.

(Local Action)

- Locally this fulfils the requirement for a PSII.
- Consideration should be given to appointing a recognised and approved external Investigator.
- CPST make further contact with Police to clarify investigation status and any restrictions for commencing contact with staff involved.

Stage 3 – Independent Investigations Review Group (IIRG)

There is an IIRG in each NHSE Regional Investigations Team to review and determine cases that require independent investigations. They have representation from experts in mental health, investigation as well as lay members. NHSE will, on receiving the Trust's commissioned investigation record, make arrangements for a review by the IIRG to take place to consider scope and quality of the internal investigation, provide feedback and determine if an any further investigation or action is required.

Commencing a PSII (ISMR can always be undertaken)

There is no automatic bar on conducting independent investigations whilst criminal investigations are underway and there should be an early discussion with relevant partners (Police and Coroner) to ensure investigations can commence at the earliest opportunity. The Regional Team then informs the Trust of the IIRG decision and what level of investigation is needed.

The regional investigations team will ensure families of the both the perpetrator and the victim are fully informed about the investigation, what they can expect from it and how they can contribute to it and seek their consent for access to medical records. They will draw up the terms of reference for the independent investigation following liaison with all appropriate stakeholders and a tender process takes place for the most suitable investigator.

Contact with families of victims and perpetrators.

Where appropriate the PSII investigator, or the Patient and Family Liaison Officer (FLO) or designated, will contact families of victim and perpetrator, this will be done with advice from and, in conjunction with, NHSE and the police.

Check in with police if any signposting has taken place for families i.e., hundredfamilies.org, or other support information shared.

The purpose of this contact is to offer condolences / sympathies on behalf of the Trust and to explain the Trust PSII process to relatives as part of the Trust Compassionate Engagement with Patients, Families and Staff following a Patient Safety Incident: Guidance for Staff.

Support for staff (in addition to 'The Post-Incident Pathway for Staff Support (PIPSS) Policy' (2024))

The impact of a mental health-related homicide on the staff involved can be far-reaching. People react in different ways, and it is important to keep track of delayed or repressed responses by the staff involved.

Soon after the incident, it is helpful to hold a debrief session with the teams who cared for the alleged perpetrator. This is an opportunity to share experiences in a safe environment.

This meeting is separate from the internal investigation and is an opportunity for staff to talk through the incident. Ensure that staff involved are offered appropriate support via individual and team debriefs, followed by further referrals to other support as necessary.

Support will also be required for those staff who may also know the victim. This mix of informal and formal support should then continue at team and individual supervision.

It is important that line managers are aware and supported to create time to listen and help staff to reflect on their practice and will also option to undertake Occupational Health services and counselling services referrals for staff.

The process of investigating a mental health- related homicide can be lengthy with often high expectations around the evidence within the report and sharing the learning needs to be planned and executed with care and attention. It is important to provide regular communication and updates during this difficult time and understanding where they are in the process and what the next steps are can be helpful.

Incidents involving Infection Prevention Control (including Healthcare Associated Infections(HAI))

Staff must report all incidents pertaining to infection prevention and control in accordance with LPT reporting procedures; this includes non-adherence with infection prevention and control procedures. This automatically alerts the Infection Prevention & Control Team (IPCT) who will take appropriate action. Any additional information can be obtained directly from the IPCT.

Criteria for defining an infection prevention control incident include but are not limited to:

- Adverse effect on the activity of Inpatient Beds
- Closure of beds
- Cancellation of procedures
- Failure to comply with infection prevention and control policies and guidelines.
- Increased incidence/outbreak of infection.
- Death associated with Clostridium *difficile* (C.Diff).
- Outbreaks of Clostridium *difficile.*
- Death associated with Methicillin-resistant Staphylococcus aureus Bacteria (MRSA).
- MRSA Bacteraemia.
- Water management issues.
- Legionella.
- Sharps injuries.
- Clusters/increased incidents/outbreaks of Covid-19.
- Nosocomial infection developed during LPT care delivery.
- Environmental/Decontamination issue.

In addition to incident reporting, Patient Safety Incident reviews should be undertaken for the following for the purpose of learning and to include identifying any system failures or care delivery problems:

- Toxin positive Clostridium *difficile.*
- Death associated with Clostridium *difficile.*
- Death associated with MRSA.
- Bowel surgery associated with Clostridium *difficile.*
- MRSA Bacteraemia.
- Increased incidence/outbreak of infection resulting in closure of a ward.
- Death directly related to Covid-19.
- Death directly related to a nosocomial infection.

Patient National Screening Incidents

National screening programmes are public health interventions, which aim to identify disease or conditions in defined populations to either reduce morbidity or mortality. Screening programmes are sometimes made complicated because the activity of screening often takes place within pathways across several organisations/healthcare providers.

These incidents should be reported via Ulysses and then directly reported to for Public Health Commissioning teams (PHCTs) for Screening following a specific investigation pathway; CPST will facilitate this process and provide specialist advice and next steps management required by the clinical teams involved following national Specialist Commissioners for Screening advice.

This usually involves the completion of a ‘Screening Incident Assessment Form’ available from NHSE Screening Quality Assurance Service (SQAS). Further

information can be found on the screening programmes at https://www.gov.uk/government/publications/managing-safety-incidents-in-nhs-screening-programmes.

There is online guidance/flowchart for 'Reporting and managing screening incidents flowchart' which can be found at: https://www.gov.uk/government/publications/managing-safety-incidents-in-nhs-screening-programmes/reporting-and-managing-screening-incidents-flowchart

Data Privacy/Data Protection Team

- In the event of an incident involving security of information the Information Governance (IG) / Data Privacy Team will be responsible for assessing the incident category and notifying relevant external bodies and appropriate key staff and organisations in line with Department of Health Guidance/ Information Commissioner Office (ICO) if it is considered to have met the threshold for notifiable IG breach.
- The immediate response to an IG incident and the escalation process for reporting and investigating will vary according to the severity of the incident.
- If it is established the IG incident includes patient identifiable information/data that has been lost or inappropriately placed in the public domain, patients should be informed as soon as possible and an apology given, and any action taken. Where there is any risk of identity theft it is strongly recommended that this is done as soon as possible even before completion of an ISMR has been completed.
- The Trust has adopted the NHS Digital published data breach guidance to support these mandatory requirements and all reporting is based on this guidance. With the support of the CPST the use of a designated 48-hour Data Breach Initial Service Manager Review (ISMR) has been developed to capture as much information as possible about the incident and to assist the Data Privacy Team in determining whether it meets the 'reportable' criteria against the set of national standards used by the ICO.
- The Guidance for process and assessment of the severity of the incident can be found in **Appendix 6.**

Information Technology (IT) Incidents

The immediate response to the incident and the escalation process for reporting and investigating will vary according to the severity of the incident and will be managed in conjunction with IT Senior Managers; this may also include LPT Clinical Safety Officers.

- The Guidance for process and assessment of the severity of the incident can be found in **Appendix 7.**

Overview of External Stakeholders who may influence/request incident investigation information and responses at LPT.

Area of concern	Responsible Body	Reporting Responsibility
Patient Safety Incident Investigations	Relevant ICB/Specialist commissioners/Collaboratives	CPST - Head of Patient Safety. Incident Investigation Corporate Lead. CPST Lead Nurse.
Never Events Homicide National Screening Incidents	Relevant ICB/ Specialist commissioners/Collaboratives, CQC,	CPST - Head of Patient Safety. Incident Investigation Corporate Lead. CPST Lead Nurse.
Request to conduct incident investigation - linked to national priorities.	Health Services Safety Investigations Body (HSSIB) (formerly the Healthcare Safety Investigation Branch)	CPST - Head of Patient Safety. Incident Investigation Corporate Lead. CPST Lead Nurse.
Medical Devices	Medicines and Healthcare Products Regulatory Agency (MHRA)	LPT Trust Lead - Medical Devices Lead/Medical Devices Safety Officer, Clinical Safety Officers. Head of Patient Safety Incident Investigation Corporate Lead CPST Lead Nurse
Medicines	Medicines and Healthcare Products Regulatory Agency (MHRA) National Safety Alerts	LPT - Medicines safety officer/Chief Pharmacist, CPST - Lead Nurse
Reporting of Injuries, Diseases and Dangerous Occurrences (RIDDOR)	Health and Safety Executive	Trust Lead - Lead for Health and Safety Compliance CPST - Incident Investigation Corporate Lead. CPST Lead Nurse
Litigation/Claims	NHS Resolution	Director of Corporate Services/Claims Manager

Unexpected death of patient/Responses to Regulation 28 Recommendations	H M Coroner and H M Coroner's Officers	Trust Lead - Quality and Compliance Head of Patient Safety. Incident Investigation Corporate Lead. CPST Lead Nurse.
Media interest	The Media	Trust Communications Lead and Chief Executive or nominated Deputy
NHS National Safety alerts	NHS Central Alert System	Coordination through CPST - Head of Patient Safety & Lead Nurse. Trust nominated Central Alerts System (CAS) Officer
Criminal matters	Police	Security Management Advisors
Fire related issues	Leicestershire Fire and Rescue	Head of Health & safety Compliance. Fire Officer/ Health & Safety Advisors.
Safeguarding	Leicestershire County Council/ Local Authority (Relevant ICB/Specialist commissioners/Collaboratives)	Trust Head of Safeguarding /Lead Practitioners Nominated Deputy Director of Nursing & Allied Healthcare Professionals
Estates and Facilities. Environment Agency.GOV.UK	NHSE Estates & Facilities (NHS Property Services)	Trust Lead - for Estates and Facilities or nominated deputy
Copies of independent investigation reports by external agency	Care Quality Commission NHSE HSSIB	Executive Director of Nursing/AHP's /Chief Executive CPST - Head of Patient Safety Incident Investigation Corporate Lead/ Lead Nurse
Audit information on suicides and homicides	National Confidential Enquiry into Suicide and Homicide by People with Mental Illness	Trust Suicide Prevention Lead in conjunction with Directorate of Mental Health

		Safeguarding Team
Information Governance/Data Privacy	Information Commissioners Office (ICO). NHS Digital (NHSE)	Trust Data Privacy Lead. Trust Information Technology Lead/ LHIS
Security incidents (including Fraud) Digital/Cyber	NHS Counter Fraud Service (NHSCFA) NHS Digital/Cyber (NHSE)	Trust Security Management Advisor & Fraud Advisor Cyber Security Lead. Trusts Information Technology Lead/ LHIS. Clinical Safety Officers
Unexpected death of patients under a section of the Mental Health Act 1983	Care Quality Commission	The Trust Mental Health Act Manager in conjunction with Directorate of Mental Health & nominated Trust Executive Lead Trust Quality & Compliance Team
General Medical Council (GMC)	Concerns in relation to medical staff practice/conduct	The Medical Director. Director of Human Resources
Health and Care Professions Council (HCPC)	Concerns in relation to practice of allied healthcare professionals	Executive Director of Nursing and Quality/AHP's or delegated deputy Director of Human Resources
Nursing and Midwifery Council (NMC)	Concerns in relation to nursing/nursing associate staff practice / conduct	Executive Director of Nursing and Quality/AHP's or delegated deputy

The above list is not exhaustible.

Records Management and Confidentiality

Incident report forms are sensitive documents, should be considered confidential, and must be stored securely. The Trust has a legal obligation to retain incident forms for a minimum period of 10 years. Incident forms relating to the under 18's should be retained for a period of 25 years.

Incident forms should not be printed out/uploaded to a patient's healthcare record and must not be filed in patient notes.

It is essential to record that there has been an incident in the patient record including the incident number and the discussion that has taken place at the time with the patient/family in relation to the incident.

Incident forms can become the subject of internal and/or external scrutiny and must be completed to the same standards of accuracy with objective, factual description as expected in the clinical record.

Any written information produced as part of the LPT incident reporting process will be potentially disclosable under the Freedom of Information Act 2000 ("FOIA"), unless an exemption applies to the information and can be requested by H M Coroner Inquests, complaints, claims etc. It is essential that incident forms are completed accurately and that all relevant information relating to the incident is documented. The information recorded on the incident form should be factual and accurate; supposition, inappropriate opinion or unverifiable facts should not be recorded.

Incident forms can contain sensitive patient and staff related information. As such, the Trust has a duty of care in relation to confidentiality and a legal obligation in relation to the General Data Protection Regulations (GDPR) from 25 May 2018 and the Data Protection Act 2018 placing a responsibility to ensure that all such sensitive personal data is stored in a secure location.

Incident Reporting Business Continuity

In the event of the electronic database 'Ulysses' failing delaying the reporting of incidents to beyond a staff member's completed shift staff should report the incident to their line manager by email and agree who will complete the incident report at the next opportunity. Escalation/investigation into the incident and informing patients/families should not be delayed as a result because of an interruption to the system.

The failure of the reporting system will be reported to Ulysses at the earliest opportunity by CPST in collaboration with the Quality and Compliance Team.

To summarise

As part of the Trust's provision as an NHS provider of care and commitment to keep patients and staff safe it is required by the CQC to have:

- A robust incident reporting system and processes to support the early identification, reporting, investigation, and escalation as required.
- Be able to identify and learn from incidents locally and across the healthcare community by supporting the LFPSE.

- To support the planning of services and review of risks associated with incident reporting.
- To support the identification of safety themes, linking into the complaints and patient feedback process and helps inform the Trusts Legal team in the likelihood of a claim against the Trust.

5.0 Consent

Clinical staff must ensure that consent has been sought and obtained before any care, intervention or treatment described in this policy is delivered. Consent can be given orally and/ or in writing. Someone could also give non-verbal consent if they understand the treatment or care about to take place. Consent must be voluntary and informed, and the person consenting must have the capacity to make the decision.

In the event that the patient's capacity to consent is in doubt, clinical staff must ensure that a mental capacity assessment is completed and recorded. Someone with an impairment of or a disturbance in the functioning of the mind or brain is thought to lack the mental capacity to give informed consent if they cannot do one of the following:

- Understand information about the decision.
- Remember that information.
- Use the information to make the decision.
- Communicate the decision.

6.0 Monitoring Compliance and Effectiveness

Monitoring tools must be built into all procedural documents in order that compliance and effectiveness can be demonstrated.

Be realistic with the amount of monitoring you need to do and time scales.

Page/Section	Minimum Requirements to monitor	Method for Monitoring	Responsible Individual /Group	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group). Frequency of monitoring
17	Outstanding incidents that remain unclosed/reviewed by local managers	Weekly reports run by CPST shared to key individuals into all directories.	Directorate Heads of Nursing/Service Leads	To Executive board monthly/bi-monthly. Monthly into Incident Oversight Group (IOG) Local Directorate Quality & Safety Groups.
16	Incomplete/saved for later incidents reports	IOG	CPST for sharing monthly report to directorate governance teams	IOG
16	Returned for updating due to PID/SID in main body of incident report	IOG	CPST for sharing monthly report to directorate governance teams	IOG

7.0 References and Bibliography

The NHS Patient Safety Strategy (2019) https://www.england.nhs.uk/patient-safety/the-nhs-patient-safety-strategy/

Patient Safety Incident Response Framework (2022) updated July 2024. https://www.england.nhs.uk/publication/patient-safety-incident-response-framework-and-supporting-guidance/

Patient safety incident response plan (PSIRP) 2023-2024 https://www.leicspart.nhs.uk/wp-content/uploads/2023/11/LPT-PSIRP-Sept-2023-FINAL.pdf

Learn from patient safety events (LFPSE) service https://www.england.nhs.uk/patient-safety/patient-safety-insight/learning-from-patient-safety-events/learn-from-patient-safety-events-service/

Post-Incident Pathway for Staff Support (PIPSS) Policy **(2024)**
Can be found on the trust website

Infection Prevention and Control Assurance Framework Policy (2023)

Can be found on the trust website

Guidance: Managing safety incidents in NHS screening programmes (2015 last updated October 2024) https://www.gov.uk/government/publications/managing-safety-incidents-in-nhs-screening-programmes

https://www.gov.uk/government/publications/managing-safety-incidents-in-nhs-screening-programmes/reporting-and-managing-screening-incidents-flowchart

A Culture of Candour Policy (Incorporating 'Being Open' and 'Duty of Candour) (2022)

Health and Safety Policy (2022)

Data Protection and Information Sharing Policy:(incorporating Confidentiality, Information Sharing, Safe Haven and Pseudonymisation procedures) (2021)

Information Security and Risk Policy (2023)

Freedom to Speak Up Policy: Speak up, Listen up, Follow up (2023)

https://www.cqc.org.uk/guidance-providers/regulations-enforcement/regulation-20-duty-candour

www.hse.gov.uk/riddor/ Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR)

www.mhra.gov.uk Medicines and Healthcare Products Regulatory Agency (MHRA)

https://ico.org.uk/ (Information Commissioners Office)

Public Interest Disclosure Act 1998, Chapter 23. London: The Stationery Office. Available at: www.opsi.gov.uk

Department of Health. (1998). Health Service Circular 1999/198, The Public Interest Disclosure Act 1998: Whistle blowing in the NHS. London: Department of Health. Available at www.dh.gov.uk/

https://improvement.nhs.uk/resources/just-culture-guide/

If a patient commits a homicide: A resource for psychiatrists (June 2024) https://www.rcpsych.ac.uk/docs/default-source/improving-care/better-mh-policy/college-reports/guidance-booklet---staff-support-following-patient-homicide.pdf?sfvrsn=540ba062_9

https://www.england.nhs.uk/london/our-work/mental-health-support/homicide-support/

https://www.tewv.nhs.uk/wp-content/uploads/2021/10/Incident-recording-and-response-policy.pdf

Mental Health-Related Homicide Information for Mental Health Providers April 2019

https://www.england.nhs.uk/london/wp-content/uploads/sites/8/2019/08/Information-for-Mental-Health-Providers_V4.0.pdf

https://www.hundredfamilies.org/

Care Act 2014. https://www.legislation.gov.uk/ukpga/2014/23/section/42

Information related to Section 42 - https://www.llradultsafeguarding.co.uk/enquiries-under-section-42/

https://www.cqc.org.uk/guidance-regulation/providers/notifications

8.0 Fraud, Bribery and Corruption consideration

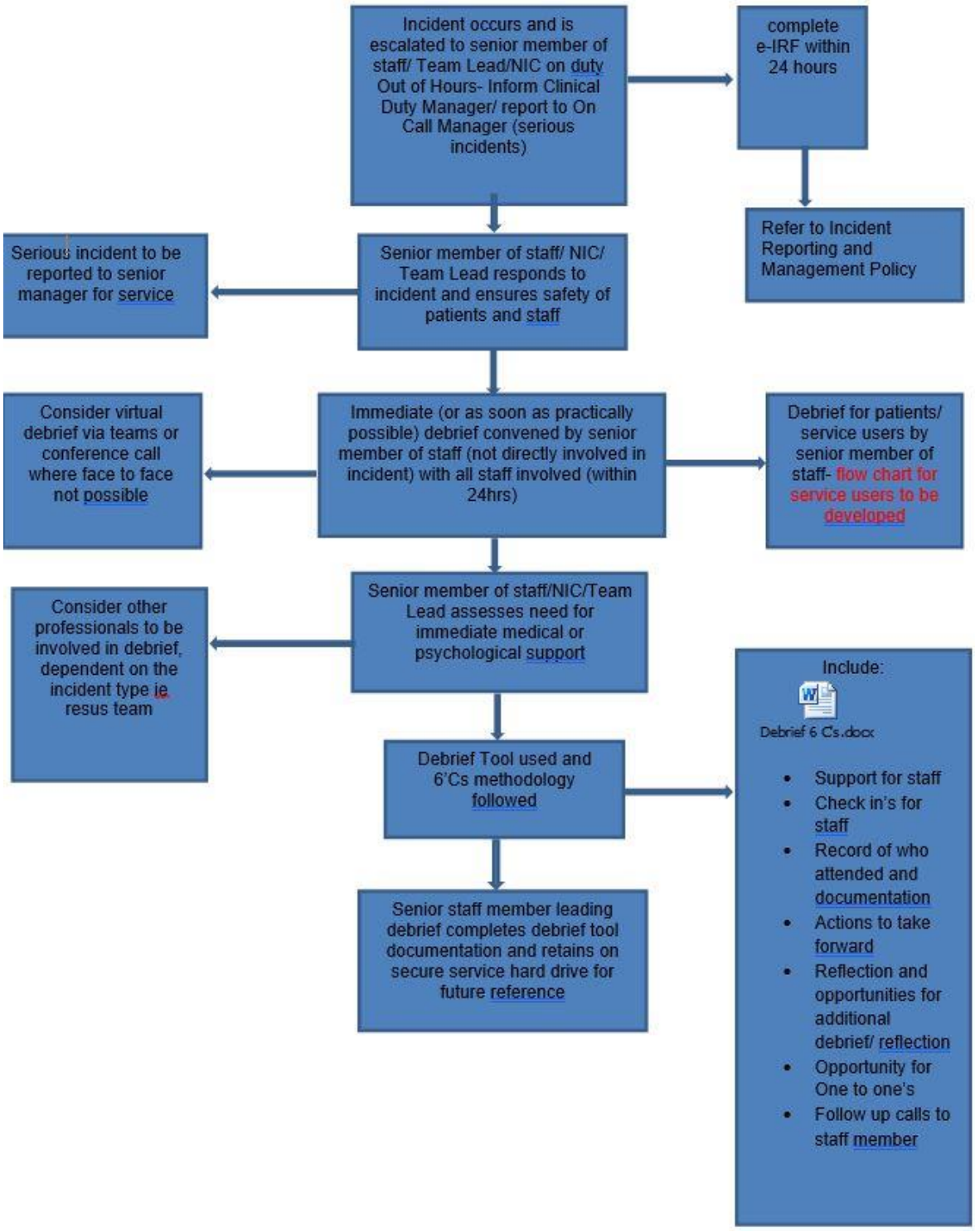
The Trust has a zero-tolerance approach to fraud, bribery, and corruption in all areas of our work and it is important that this is reflected through all policies and procedures to mitigate these risks.

Fraud relates to a dishonest representation, failure to disclose information or abuse of position to make a gain or cause a loss. Bribery involves the giving or receiving of gifts or money in return for improper performance. Corruption relates to dishonest or fraudulent conduct by those in power.

Any procedure incurring costs or fees or involving the procurement or provision of goods or service, may be susceptible to fraud, bribery, or corruption so provision should be made within the policy to safeguard against these.

If there is a potential that the policy being written, amended or updated controls a procedure for which there is a potential of fraud, bribery, or corruption to occur you should contact the Trusts Local Counter Fraud Specialist (LCFS) for assistance.

Appendix 1 - Debrief Flow Chart following an incident- Staff Members



Appendix 2 - Provision of Staff Welfare and Support – Debrief Tool

Leicestershire Partnership NHS Trust

Provision of Staff Welfare and Support

Debrief Tool

Introduction

A debrief can be described as an opportunity for staff who have been involved in an incident to reflect on what has happened, identify a way forward and be offered support. Following an incident, there is often a pull to 'do something', however, the evidence for debriefing is mixed and, in some cases, a debrief can be harmful. Staff often ask for a debrief session, but it must be acknowledged that not everyone will feel comfortable with this and the debrief must be optional. This tool has been developed as part of the Trust's Guidelines for the Provision of Staff Welfare and Support following an incident. It is designed to help team members to facilitate a debrief for colleagues after an incident. The tool is based on the 6Cs - values which all NHS staff are encouraged to embrace.

How to use this tool

This tool aims to provide a structure for the debrief process and some ideas for discussion points (you may wish to add your own ideas). The document will also provide a record of the debrief and highlight ongoing actions you have identified.

	Discussion Points	Notes and Actions
1. Care *Care is our core business and that of our organisations and the care we deliver helps the individual person and improves the health of the whole community. Caring defines us and our work. People receiving care expect it to be right for them consistently throughout every stage of their life.*	• How is everyone feeling? (physically/emotionally?) • What did that experience feel like? • What do you think will help you now?	

	Discussion Points	Notes and Actions
2. Compassion *Compassion is how care is given through relationships based on empathy, respect and dignity.* *It can also be described as intelligent kindness and is central to how people perceive their care.*	• Did you feel supported following the incident? • How has the team supported each other? • How have patients and carers been supported? • How can we understand this from the involved patient's perspective?	
3. Competence *Competence means all those in caring roles must have the ability to understand an individual's health and social needs. It is also about having the expertise, clinical and technical knowledge to deliver effective care and treatments based on research and evidence.*	• What went well and not so well? • Was everyone's training up to date i.e. SCIP, MAPA, safeguarding etc.? • Was there anything that you feel may have contributed to the incident i.e. staffing shortage etc.?	
4. Communication *Communication is central to successful caring relationships and to effective team working. Listening is as important as what we say and do. It is essential for "no decision about me without me".* *Communication is the key to a good workplace with benefits for those in*	• What was handed over to you regarding this patient? • Were you aware of the care plan or risk assessment that was in place? • What was your role in the incident?	

	Discussion Points	Notes and Actions
our care and staff alike.		
5. Courage *Courage enables us to do the right thing for the people we care for, to speak up when we have concerns. It means we have the personal strength and vision to innovate and to embrace new ways of working.*	• Did you feel you had the courage to say if you didn't agree with the approach taken? • Did you feel safe at the time? • Did you feel confident in your role at the time?	
6. Commitment *A commitment to our patients and populations is a cornerstone of what we do. We need to build on our commitment to improve the care and experience of our patients.*	• Reflecting on the incident, is there anything that you think could have been done differently? • What are our learning points? • What do we need to do to prevent or manage these types of incidents in the future?	

Next steps - checklist

☑ Let participants know that their emotional response is an expected part of the adjustment process to the experience of trauma, and mild symptoms are likely to subside over the coming weeks. After four weeks, anyone still experiencing symptoms should seek further support, for example your GP, occupational health or Amica.

☑ Identify any follow up actions.

☑ Identify support needs of other staff, patients, witnesses or relatives who may have been affected by the incident.

☑ Ensure all documentation is completed, including an eIRF.

Date of Debrief

……

Incident Reference

……

Facilitator:

……

Participants:

……

Appendix 3 - Guidance for staff when: 'Immediate Safety/Care issues are identified following an incident/event that signifies an unexpected level of risk / harm and/or potential for learning and improvement'. *Waiting for the next Trust IRLM is not appropriate.*

Action to be taken:

When a patient safety incident/event is reported that signifies an unexpected level of risk / harm and/or potential for learning and improvement notification. Below describes examples to consider (clinical judgement should always be applied for other incidents):

- Homicide.
- Inpatient death of a patient under the Mental Health Act (1983), community patient under a community treatment order (CTO). CTO is an order made by a responsible clinician to give you supervised treatment in the community.
- Unexpected inpatient death of a patient on a mental health ward.
- Event does not allow the Trust to continue its day-to-day business or there is significant interruption to service delivery.
- Significant information governance breach involving many patients/staff's data.
- The incident/event is notified to the Trust through other means i.e., coroner due to family concerns, media.

The most senior directorate staff member responsible for the service(s) at the time of notification should take through the following approach after ensuring local service responses have taken place:

- Notify the Executive Nurse (or designated deputy) and Trust Medical Director (or designated deputy) and share known information of the event/incident.
- If out of hours – contact Executive Director on call and Directorate senior manager and share known information of the event/incident.

From this initial information sharing a response to next step planning can be made i.e., who needs to be present at Multi-Disciplinary Team (MDT) planning meeting (this may include calling Trust 'experts' (i.e., safeguarding, Security, Data Privacy, Estates Lead).

In hours

MDT meeting will need to be arranged usually over MS Teams, chaired by the Executive Nurse, or designated Deputy and Trust Medical Deputy or designated deputy, representative from senior corporate patient safety team (CPST), member of senior nursing/manager, clinical governance team member for responsible directorate, and any identified 'specialist'.
At the MDT, the incident will be reviewed with initial known details and next steps agreed. Output from this meeting includes:

- Ensuring the event/incident is recorded on the Trusts' incident reporting system Ulysses.
- An initial senior directorate response lead will be delegated to undertake /oversee the initial service managers review and respond within 48hrs to this

and return to CPST to share with MDT meeting leads.

- Consider the response to patient(s), families, and staff and who is responsible for this.
- All actions will be recorded on Ulysses under contact tab and summarised in email titled ‘MDT ACTION and Ulysses number’ with actions allocated to and by time/date.
- Consider if Trust Communication Team need to be included to assist with external correspondence with media depending on type of incident.
- A proportionate learning response maybe agreed, i.e., it meets PSII level of review before IRLM (and incident come to IRLM ahead of the usual timeframe)
- All discussion and decisions will be recorded on Ulysses by a member of CPST.
- The patient safety incident initial findings will go on to be presented at the next available IRLM for governance completeness.
- All email correspondence, subsequent meetings in directorate in relation to response will be stored on Ulysses.
- Outcome of the meeting will include communication response with appropriate external stakeholders ‘ i.e., ICB/Commissioners/CQC/NHSE.

Out of hours

Contact Executive Director on call out of hours and Directorate senior manager and share known information of the event/ incident. Responsibility includes:

- Ensuring the event/incident is recorded on the Trusts’ incident reporting system Ulysses.
- Consider the response to patient(s), families, and staff and who is responsible for this.
- An MDT planning meeting should be convened at the earliest possible time to determine next steps.
- Notification to CPST by email, copying in respective clinical governance generic email and key senior directorate staff (they may need to be notified before return to work) of all actions taken.

Convening of an MDT planning meeting should take place as soon as practicable and be recorded on Ulysses as above ‘in hours’ guide.

Immediate Safety/Care issues are identified following an incident/event that signifies an unexpected level of risk / harm and/or potential for learning and improvement.

Incident happens and is reported on Ulysses and escalated through directorate governance.

The most senior directorate staff member responsible for the service(s) at the time of notification should

In Hours

Notify the Executive Nurse (or designated deputy) and Trust Medical Director (or designated deputy)

Out of Hours

Contact Executive Director on call out of hours and Directorate senior manager

Convening of an MDT planning meeting should take place as soon as practicable and be recorded on Ulysses as above 'in hours' guide.

MDT Huddle

Called by MD/DoN or deputy(ies) to include directorate senior staff, CPST and 'experts' as required (i.e., Safeguarding, Security, Comms Team)

Agree next steps and reporting.

ISMR allocated for completion within 48hrs.

Agree reporting timescales and responsibilities based on risk to

- CQC
- ICB/Commissioners
- NHSE (for Homicide)

NB up to and before 10 days

Records of communication, decisions and escalation must be kept on Ulysses.

Appendix 4 – Examples of Incidents, this details regularly, and expected types of incidents staff should report: (not an exhaustive list)

- **Accidents:** Slips, trips & falls, cuts, burns, bumps, muscular strains, manual handling injuries, car accidents.

- **Clinical Incidents:** Error or mishap in clinical procedure, incorrect prescription or administration of drugs, absconding patients, self-inflicted injuries, incidents leading to increased length of stay, or unplanned readmission, sharps injury.

- **Violent/Unsociable Behaviour:** Assault (physical, verbal, or sexual), violent, aggressive, or severely disruptive behaviour by patients, staff or a member of the public, theft, and damage to property.

- **Hate incidents:** an incident which may or may not be a crime of abuse in any form including but not exclusively physical violence, verbal abuse, damage to property, where the victim or other persons perceive the act to have been motivated by prejudice of hostility towards any aspects of a person's identity e.g. Disability, gender identity, race, ethnicity, nationality, religion, faith, belief, sexual orientation or alternative sub cultures.

- **Dangerous Occurrences:** Electrical or mechanical faults, fire (including false alarms), equipment malfunction or failure which may result in risks to employees, patients, visitors or contractors, spillage of hazardous substances or explosions.

- **Medical Devices** (e.g., Catheters, Dressings, Endoscopes, Examination gloves, Hospital beds, Implants – powered and non-powered, Incontinence products, Intravenous administration sets and pumps, Ophthalmic equipment, Patient monitoring

- **Equipment**: (e.g., cardiac monitors), Physiotherapy equipment, , Sphygmomanometers, Surgical instruments and equipment, Syringes and needles, Thermometers, Urine drainage systems)

- **Electronic Systems & Platforms:** i.e., in relation to electronic systems/ platforms/Apps used in patient's care – such as SystmOne/AirMid/ PhotoApp/ ChatHealth/WellSky to name those currently in use and other such as electronic rota's, staff booking systems

- **Any adverse incident** involving a device or its instructions for use, especially if the incident has led to or, were it to occur again, could lead to:

    - Death, life-threatening illness, or injury
    - Deterioration in health or permanent impairment of body structure or function
    - The necessity for medical or surgical intervention (including implant revision)
    - Hospitalisation or prolongation of existing hospitalisation

- Unreliable test results and associated risk of misdiagnosis or inappropriate treatment.
- Ongoing faults that successive service/maintenance visits have failed to rectify.

If a staff member submits a report form to the MHRA, a unique reference number will be generated; this should be reported to the CPST. Any staff member can report to MHRA; however, a coordinated centralised reporting is preferred. Reporting to MHRA should not be seen as a negative outcome to an incident; it should be seen as escalation of reducing potential risk to the next patient or staff member and for the wider learning in the NHS and beyond and for informing others.

Appendix 5: Further information related to 'the reporting of injuries, diseases, and dangerous occurrences regulations 2013' (RIDDOR) reportable incidents.

The following must be reported under RIDDOR by the line manager to the Trust Health and Safety Team without delay who will report to the Health & Safety Executive (HSE); and the Incident reported via Ulysses.

- A death or major injury of any person as a result of an accident arising out of or in conjunction with work, for example where serious systematic failures in arrangements for delivery of care indicate significant failure to manage health and safety, and service users are exposed to a high level of risk including death or major injury.
- Any person "at work" and not employed by another company/organisation sustaining reportable major injuries as a result of an accident arising out of or in connection with work, including:

a) Fracture diagnosed by a registered medical practitioner of any bone except fingers, thumbs, or toes.

b) Amputation of arm, hand, finger, thumb, leg, foot or toe.

c) Injury diagnosed by a registered medical practitioner as being likely to cause permanent blinding or reduction in sight in one eye or both eyes.

d) Crush injury to the head or torso causing damage to the brain or internal organs.

e) Burn injury (including scalping) which covers >10% of the whole-body surface OR causes significant damage to the eyes, respiratory system, or other vital organs.

f) Loss of consciousness resulting from head injury or asphyxia.

g) Any degree of scalping requiring hospital treatment.

h) Injury arising from working in an enclosed space which leads to hypothermia or heat-induced illness OR requires resuscitation or admittance to hospital for > 24 hours.

People not at work (patients, visitors, etc.)

Work related accidents resulting in the person being taken directly to hospital from the scene of the accident for treatment* in respect of the injury; (*examinations and diagnostic tests do not constitute "treatment" in such circumstances) OR a "specified injury" a-h listed above if the injured person is already at a hospital.

There is no requirement to report incidents where people are taken to hospital purely as a precaution when no injury is apparent.

- Any dangerous occurrence, i.e.:

a) Collapse, overturning or failure of load bearing parts of lifts and lifting equipment.

b) Electrical incidents causing explosion of fire resulting in stoppage of plant for >24 hours OR cause significant risk of death.

c) Exposure to biological agents likely to cause severe human infection or illness i.e., sharps injury from a source patient known to have a positive blood borne infection.

- An employee or other person at work is away from work or unable to perform their normal duties for more than 7 consecutive days as a result of a physical injury caused by an accident at work.

- If a doctor (or occupational health service doctor) notifies the line manager that their employee has a diagnosis of a reportable disease and the employee undertakes work that links with that condition, it must be reported under reportable disease e.g., some skin diseases, cancers, occupational asthma, hepatitis, and certain musculoskeletal disorders – seek advice from the Trust Health & Safety Compliance Team.

- The death of an employee if this occurs sometime after the reportable injury that led to the employee's death, but not for more than one year afterwards.

Please contact the Health, Safety and Compliance Team for further information and retain RIDDOR reports for minimum of 10 years.

Appendix 6 - Guide to the notification of data security and protection incidents. (Dept of Health and Social care - May 2018)

Overview

The General Data Protection Regulation (GDPR) as implemented by the UK Data Protection Act 2018 came into UK Law on 25 May 2018. It introduced a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. The Security of Network and Information Systems Directive ("NIS Directive") also requires reporting of relevant incidents to the Department of Health and Social Care as the competent authority from 10 May 2018.

An organisation must notify a breach of personal data within 72 hours. If the breach is likely to result in a high risk to the rights and freedoms of individuals, organisations must also inform those individuals without undue delay.

Organisations should ensure robust breach detection, investigation, and internal reporting procedures in place. This will facilitate decision-making about whether, or not, you need to notify the relevant supervisory authority and the affected individuals.

It remains a contractual requirement of health and social care organisations using the standard NHS contract to include statistics on personal data breaches in the annual report presented to the board.

Organisations must also keep a record of any personal data breaches, regardless of whether it is required to notify. It must not include the identity of any person involved in a data breach in a notification. The local file may contain such information, but this file will only be requested by the Information Commissioner (ICO) if further investigation is required.

This guide supersedes the ‘Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation’ (2015).

Mandate: General Data Protection Regulation as Implemented by the Data Protection Act 2018 (GDPR)

It is a legal obligation to notify personal data breaches of the General Data Protection Regulation under Article 33 within 72 hours, to the ICO, unless it is unlikely to result in a risk to the rights and freedoms of individuals. Article 34 also makes it a legal obligation to communicate the breach to those affected without undue delay when it is likely to result in a high risk to individual’s rights and freedoms. It is also a contractual requirement of the standard NHS contract to report incidents in accordance with this guidance. By notification this may be an initial summary with very little detail known at the outset but a fuller report that might follow. There is no expectation that a full investigation will be carried out within 72 hours. The Information Commissioner has asked all relevant health and social care

organisations to use this reporting tool accessed via the Data Security and Protection Toolkit in preference to the ICO provided reporting mechanism so that sector intelligence gathering and local solutions to groups of incidents can be implemented.

A processor of personal data that discovers a breach has occurred has a legal obligation to inform the controller of that personal data under Article 33(2) of GDPR as clarified in the Article 29 working party guidelines on personal data breach reporting (II, A, 3). It is possible for a processor to make a notification on behalf of the controller, but only where the controller has authorised the notification and this has been documented as part of the contractual arrangements between the controller and the processor. However, it is important to note that the legal obligation remains with the controller.

ICO currently advise the following relating to reporting health and care sector incidents - 'All health service organisations in England must now use the IG Toolkit Incident Reporting Tool. This will report IG SIRIs to the NHS Digital, Department of Health, ICO and other regulators.' (The IG Toolkit is now replaced with the Data Security and Protection Toolkit).

Personal Data Breaches - What is a breach?

A breach is defined as:

Article 4(13) "Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Breach reporting is now mandatory for all organisations. The GDPR definitions, notification and subject communication requirements will include breaches that organisations might not have notified under the previous data protection regime. The traditional view that a data breach is only reportable when data falls into the wrong hands is now replaced by a concept of a 'risk to the rights and freedoms of individuals' under Article 33 of GDPR. Any security breach that creates a risk to the rights and freedoms of the individual is a personal data breach and could be notifiable to the ICO if it reaches a certain threshold. Any personal data breach that could create a significant risk to the rights and freedoms of an individual definitely must be notified to the Information Commissioner via this reporting tool. All personal data breaches will involve a breach of security at some point in the processing and the additional use of this tool for NIS incident reporting will save the health and social care sector time and effort in reporting.

Personal data is defined as:

'Any information relating to an identified or identifiable living individual.'

And an "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to— (a) an identifier such as a name,

an identification number, location data or an online identifier, or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

This definition now makes it clear that all paper records that relate to a living individual are included in the definition and that any aspect of digital processing such as IP address and cookies. Geographical data and biometric data are also clarified as being personal data when they can also be linked to a living individual.

What are the types of breaches?

The three types of breaches as defined in the Article 29 Working Party on Personal data breach notification are (I,B,2) Confidentiality, Integrity, or Availability (CIA).

The CIA Triad

- Confidentiality breach- unauthorised or accidental disclosure of, or access to personal data
- Availability breach- unauthorised or accidental loss of access to, or destruction of, personal data
- Integrity breach - unauthorised or accidental alteration of personal data
- Confidentiality breach - Unauthorised or accidental disclosure of, or access to personal data
- Availability breach - Unauthorised or accidental loss of access to, or destruction of, personal data
- Integrity breach - Unauthorised or accidental alteration of personal data – Where a health or social care record has an entry in the wrong record (misfiling) and has the potential of significant consequences it will be considered an integrity breach.

When is an incident reportable under GDPR? Grading the personal data breach

Any incident must be graded according to the significance of the breach and the likelihood of those serious consequences occurring. The incident must be graded according to the impact on the individual or groups of individuals and not the organisation. It is advisable that incidents are reviewed by the Data Protection Officer or Caldicott Guardian or the Senior Information Risk Owner (SIRO) when determining what the significance and likelihood a data breach will be.

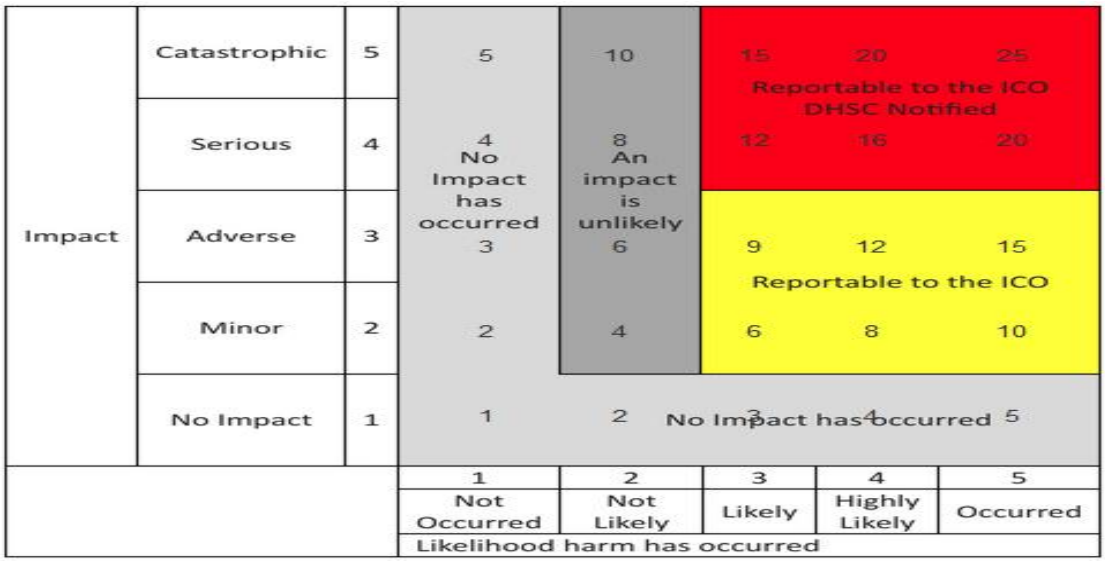
The significance is further graded rating the incident of a scale of 1-5; 1 being the lowest and 5, the highest.

The likelihood of the consequences occurring are graded on a scale of 1-5 1 being a non-occurrence and 5 indicating that it has occurred.

Where the personal data breach relates to a vulnerable group in society, as defined below, the minimum score will be a 2 in either significance or likelihood unless the incident has been contained. This will have the effect of automatically informing the Information Commissioner if one of the other axes scores above a 3.

Breach Assessment Grid

This operates on a 5 x 5 basis with anything other than “green breaches” being reportable. Incidents where the grading results are in the red are advised to notify within 24 hours.



If a breach involves certain categories of vulnerable groups, it must be scored as a minimum 2 on both axes of the scoring matrix although it may be higher depending on the severity or likelihood but will not In all circumstances be notified to the ICO:

For clarity special categories under GDPR not listed below include:

- Vulnerable children
- Vulnerable adults
- Criminal convictions/prisoner information
- Special characteristics listed in the Equality Act 2010 where not explicitly listed in this guidance and it could potentially cause discrimination against such a group or individual.
- Communicable diseases as defined by public health legislation.
- Sexual health
- Mental health

Special Categories of personal data - For clarity special categories under GDPR are:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership and the processing of genetic data.
- Biometric data for the purpose of uniquely identifying a natural person.
- Data concerning health.
- Data concerning a natural person's sex life or sexual orientation.

By criminal convictions and offenses under Article 10 of the GDPR , this has the further meaning listed in the Data Protection Act 2018 Part 2, Chapter 2, S11 (2) and is taken to include:

- The alleged commission of offences by the data subject or
- Proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

Assessing risk to the rights and freedoms of a data subject?

The GDPR gives interpretation as to what might constitute a high risk to the rights and freedoms of an individual. This may be any breach which has the potential to cause one or more of the following:

- Loss of control of personal data
- Limitation of rights
- Discrimination
- Identity theft
- Fraud
- Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy.
- Other significant economic or social disadvantage to individuals.

Depending on the outcome of the scoring matrix contained in this guide the risk may be high risk and be significant enough to notify to the ICO.

How to report an incident summary

How to report an incident? (Data Privacy Team)

Using the Data Security and Protection Reporting Tool has been designed so that organisations can report notifications of incident without having to study detailed guidance. Notifiable breaches are those that are likely to result in a high risk to the rights of freedoms of the individual (data subject). The scoring matrix used in this reporting tool has been designed to identify those breaches that meet the threshold for notification.

When to report within 72 hours

The GDPR Article 33 requires reporting of a breach within 72 hours. The 72 hours starts when an organisation becomes aware of the breach which may not necessarily be when it occurred. An organisation must have a reasonable degree of certainty that a security incident has occurred and that this has led to personal data being compromised. This means that once a member of staff or the public has reported a breach this is the point that an organisation is aware. The actual incident may have occurred some hours, days, or weeks previously, but it is only when an organisation is aware that the breach has occurred that the 72 hours to notification period starts. Where the 72 hours deadline is not met an organisation must provide an explanation. Failure to notify promptly may result in additional action by the ICO in respect of GDPR. The information needs to be gathered within 48hrs in order to clarify and grade the incident pre-submission. Local records required for an incident notified to the ICO.

A local file, which may be requested by the Information Commissioner, must be maintained which must contain the following sections:

- The facts relating to the breach.
- Its effects.
- The remedial action taken.

Communication of a personal data breach to the data subject

Article 34 of GDPR requires any personal data breach that is likely to result in a high risk to the rights and freedoms of individuals, to be communicated with those affected. Any communication must contain the following four elements:

1. A description of the nature of the breach.
2. The name and contact details of the data protection officer or other contact point from whom more information can be obtained.
3. A description of the likely consequences of the personal data breach.

4. A description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

A communication is not necessary in the following three circumstances:

1. The controller has implemented appropriate technological and organisational protection measures which were applied to the personal
2. Data affected by the breach for example the data were encrypted.
3. The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms if individuals is no longer likely to materialise.

It would involve a disproportionate effort. However, there is still an obligation to have a communication by another means such as a press notice or statement on the organisation website.

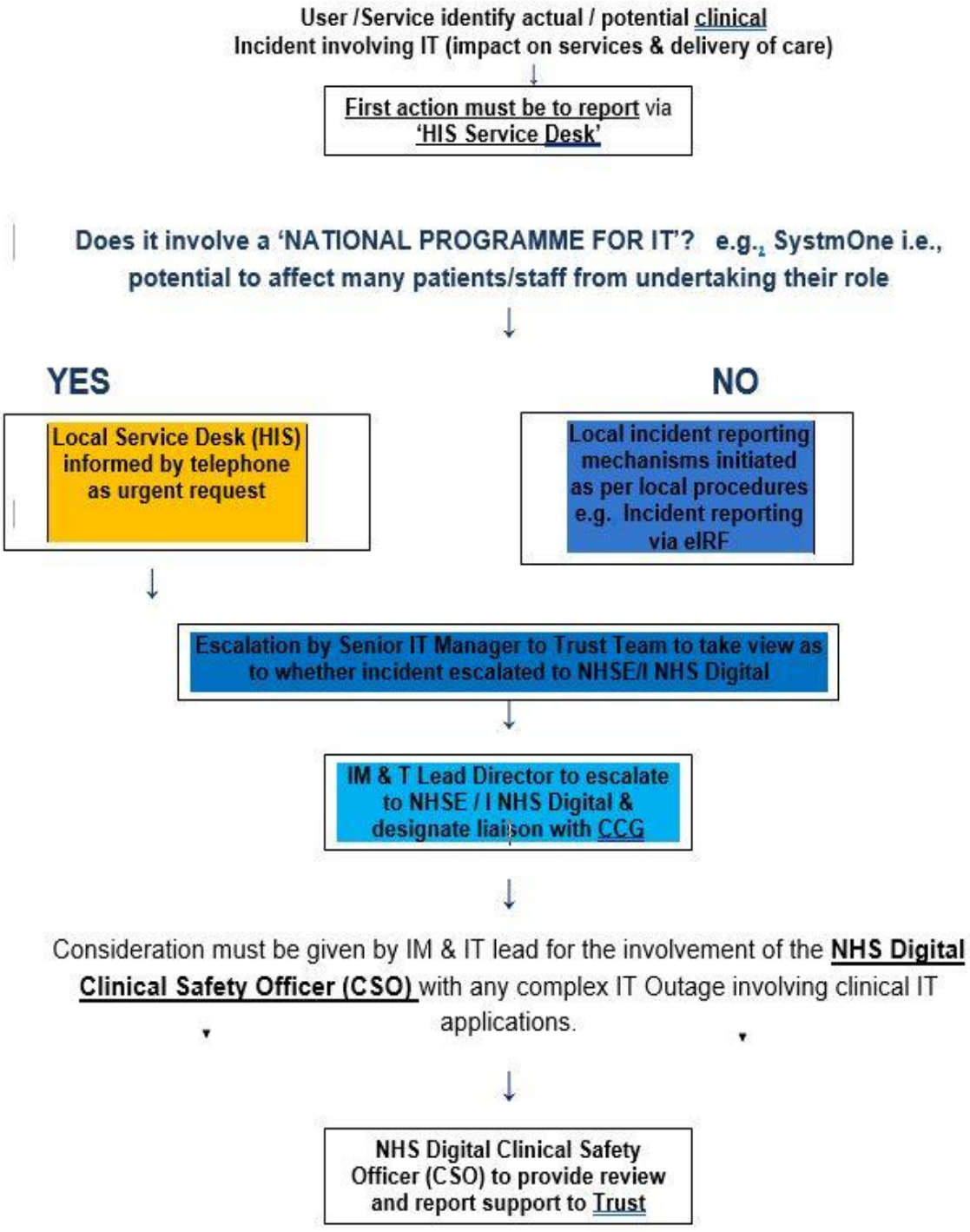
Reporting scheme for data breaches from 25 May 2018 (current for 2024)

The questions asked of organisations reporting an incident are:

ID	Information Requested
1	Organisation Name
2	Organisation Code
3	Name of the person Submitting incident
4	Email Address of person Submitting incident
5	Sector
6	What has happened
7	How did you find out
8	Was the incident caused by a problem with a network or an information system?
9	What is the local ID for this incident
10	When did the incident start?
11	Is the incident still on going?
12	Have data subjects or users been informed?
13	Is it likely that citizens outside England will be affected
14	Have you notified any other (overseas) authorities about this incident?

15	Have you informed the Police?
16	Have you informed any other regulatory bodies about this incident?
17	Has there been any media coverage of the incident (that you are aware of)?
18	What other actions have been taken or are planned?
19	How many citizens are affected?
20	Who is affected?
21	What is the likelihood that people's rights have been affected?
22	What is the severity of the adverse effect?
23	Has there been any potential clinical harm as a result of the incident?
24	Has the incident disrupted the delivery of healthcare services?
25	Which of these services are operated by your organisation?

Appendix 7 - Information technology (IT) incident management flowchart



NB: First action must always to report the incident via LHIS' and coordinating manager should consider informing the relevant directorate Clinical Safety Officer and provide details of incident including the Ulysses incident number.

Appendix 8 Training Needs Analysis

Training topic:	1. Reporting and Managing Incidents 2. Patient Safety Level 1 and 2 (National Training)	
Type of training: (see study leave policy)	Role Essential (must be on the role essential training register) *	
Directorate to which the training is applicable:	Adult Mental Health* Community Health Services * Enabling Services * Families Young People Children / Learning Disability/ Autism Services Hosted Services *	
Staff groups who require the training:	All	
Regularity of Update requirement:	3 years or as changes occur with incident reporting or systems used to manage incidents.	
Who is responsible for delivery of this training?	1. CPST & Directorate Clinical Governance Teams 2. HEE – National Patient Safety Training via e-learning on Ulearn	
Have resources been identified?	yes	
Has a training plan been agreed?	yes	
Where will completion of this training be recorded?	ULearn *	
How is this training going to be monitored?	Through Directorate local reports	
Signed by Learning and Development Approval name and date	T Ward	Date: 6th January 2025

Appendix 9 The NHS Constitution

- The NHS will provide a universal service for all based on clinical need, not ability to pay.
- The NHS will provide a comprehensive range of services.

Shape its services around the needs and preferences of individual patients, their families and their carers Answer yes to all

Respond to different needs of different sectors of the population yes

Work continuously to improve quality services and to minimise errors yes

Support and value its staff yes

Work together with others to ensure a seamless service for patients yes

Help keep people healthy and work to reduce health inequalities yes

Respect the confidentiality of individual patients and provide open access to information about services, treatment and performance yes

Appendix 10 Due Regard Screening Template

Section 1	
Name of activity/proposal	Incident Reporting and Management Policy
Date Screening commenced	Sept 2024
Directorate / Service carrying out the assessment	CPST – Enabling Services
Name and role of person undertaking this Due Regard (Equality Analysis)	Susan Arnold
Give an overview of the aims, objectives and purpose of the proposal:	
AIMS: To establish a clear and consistent approach to the reporting, investigation and management of incidents.	
OBJECTIVES: To provide a safe environment for patients, staff and visitors and apply incident reporting process to support this approach.	

Section 2	
Protected Characteristic	If the proposal/s have a positive or negative impact please give brief details **It has neutral impact on all the protected characteristics**.
Age	
Disability	
Gender reassignment	
Marriage & Civil Partnership	
Pregnancy & Maternity	
Race	
Religion and Belief	
Sex	
Sexual Orientation	
Other equality groups?	

Section 3	
Does this activity propose major changes in terms of scale or significance for LPT? For example, is there a clear indication that, although the proposal is minor it is likely to have a major affect for people from an equality group/s? Please tick appropriate box below.	
	No√
High risk: Complete a full EIA starting click here to proceed to Part B	Low risk: Go to Section 4.

Section 4
If this proposal is low risk please give evidence or justification for how you reached this decision:
This policy is a review and rewrite of the preceding policy to bring it into line with PSIRF.

Signed by reviewer/assessor	S Arnold	Date	01/10/2024
Sign off that this proposal is low risk and does not require a full Equality Analysis			
Head of Service Signed	T Ward	Date	6/01/2025

Appendix 11 Data Privacy Impact Assessment Screening

Data Privacy impact assessment (DPIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet Individual's expectations of privacy. The following screening questions will help the Trust determine if there are any privacy issues associated with the implementation of the Policy. Answering 'yes' to any of these questions is an indication that a DPIA may be a useful exercise. An explanation for the answers will assist with the determination as to whether a full DPIA is required which will require senior management support, at this stage the Head of Data Privacy must be involved.		
Name of Document:	Reporting and management of Incidents Policy	
Completed by:	S Arnold	
Job title	Lead Nurse - CPST	Date 01/10/2024
Screening Questions	**Yes / No**	**Explanatory Note**
1. Will the process described in the document involve the collection of new information about individuals? This is information in excess of what is required to carry out the process described within the document.	No	
2. Will the process described in the document compel individuals to provide information about them? This is information in excess of what is required to carry out the process described within the document.	No	
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information as part of the process described in this document?	No	
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	No	
5. Does the process outlined in this document involve the use of new technology which might be perceived as being privacy intrusive? For example, the use of biometrics.	No	
6. Will the process outlined in this document result in decisions being made or action taken against individuals in ways which can have a significant impact on them?	No	
7. As part of the process outlined in this document, is the information about individuals of a kind particularly likely to raise	No	

privacy concerns or expectations? For examples, health records, criminal records, or other information that people would consider to be particularly private.		
8. Will the process require you to contact individuals in ways which they may find intrusive?	No	
If the answer to any of these questions is 'Yes' please contact the Data Privacy Team via Lpt-dataprivacy@leicspart.secure.nhs.uk In this case, ratification of a procedural document will not take place until review by the Head of Data Privacy.		
Data Privacy approval name:	**Sue Arnold**	
Date of approval	**February 2025**	

Acknowledgement: This is based on the work of Princess Alexandra Hospital NHS Trust