

Incident Reporting and Management Policy

(Formerly part of Incident/Serious Incident Reporting policy)

This policy describes the process for reporting, investigating and managing incidents

Key Words:	Incident, Serious Incident, accident, RIDDOR Investigation, Information Governance	
Version:	1.1	
Adopted by:	Trust Policy Committee	
Date this version was adopted:	24 January 2022	
Name of Author:	Susan Arnold – Patient Safety Lead Nurse Tracy Ward-Head of Patient Safety	
Name of responsible Committee:	Patient Safety Improvement Group (PSIG)	
Please state if there is a reason for not publishing on website:	N/A	
Date issued for publication:	January 2022	
Review date:	June 2023	
Expiry date:	August 2024	
Target audience:	All Staff	
Type of Policy	Clinical X	Non Clinical X
Which Relevant CQC Fundamental Standards?	Regulation 12, 13, 20	

Contents

Version Control.....	4
Equality Statement.....	5
Due Regard.....	5
Definitions.....	6
1.0 Introduction.....	7
2.0 Statement and Purpose of the Policy.....	7
3.0 Executive Summary.....	8
4.0 Confidentiality application to Incident Reporting.....	9
5.0 Definition of an incident.....	9
6.0 Definitions associated with Incident Reporting.....	9
7.0 Roles and Responsibilities.....	12
8.0 Quality Checking.....	15
9.0 Managing Incidents.....	18
10.0 Information Technology (IT) Incidents.....	20
11.0 Information Governance /Data Privacy Incidents and Assessing Severity.....	20
12.0 Management of incidents where more than one Department or Organisation is involved..	20
13.0 Healthcare Associated Infections.....	21
14.0 Screening Incidents.....	21
15.0 Pressure Ulcers/Tissue Viability.....	21
16.0 Inpatient Falls.....	21

REFERENCES AND ASSOCIATED DOCUMENTATION

Appendix 1 External Stakeholders.....	23
Appendix 2 Examples of Incidents.....	25
Appendix 3 RIDDOR Reporting incidents.....	26
Appendix 4 Grading of Incidents/Closure Timescales.....	27
Appendix 5 Information Technology Incidents (IT).....	28

Appendix 6	Guide to the notification of data Security & Protection incidents (Dept. of Health & Social Care May 20218)	29
Appendix 7	Factual Account for staff	36
Appendix 8	Debrief Flow Chart following an incident- Staff Members	38
Appendix 9	Provision of Staff Welfare and Support- Debrief Tool	39
Appendix 10	Due Regard Screening Template	42
Appendix 11	Training Needs Analysis	43
Appendix 12	NHS Constitution Checklist	45
Appendix 13	Stakeholder and Consultation	46
Appendix 14	Data Privacy Impact Screening Assessment	47
Appendix 15	References and Bibliography	49

Version Control and Summary of Changes

Version Number	Date	Comments (description change and amendments)
1 1.1 Ext agreed at Dec Quality Forum	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.

For further information contact:

Trust Lead – Head of Patient Safety
Leicestershire Partnership NHS
Trust Room 170,
Pen Lloyd Building County Hall
Glenfield, Leicester
LE3 8TH

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 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.

In carrying out its functions, LPT must have due regard to the different needs of different protected equality groups in their area.

This applies to all the activities for which LPT is responsible, including policy development and review and implementation.

Due Regard

LPT's commitment to equality means that this policy has been screened in relation to paying due regard to the general duty of the Equality Act 2010 to eliminate unlawful discrimination, harassment, and victimisation; advance equality of opportunity and foster good relations.

This is evidenced by incident forms being completed either electronically or on paper dependent on whether staff can access or use a computer. This policy is also available in other formats such as braille

Due regard will also be given through the use of Human Resources (HR) best practice and adherence to all relevant employment legislation.

In addition to the examples highlighted above, equality monitoring of all relevant protected characteristics to which the policy applies will be undertaken. Robust actions to reduce, mitigate and where possible remove any adverse impact will be agreed and effectively monitored.

This policy will be continually reviewed to ensure any inequality of opportunity for service users, patients, carers and staff is eliminated.

The Due regard assessment template is Appendix 10 of this document.

Definitions/Abbreviations that apply to this Policy

HSE	Health and Safety Executive
CQC	Care Quality Commission
IG	Information Governance
RCA	Root Cause analysis
RIDDOR	The Reporting of Injuries, Disease, and Dangerous Occurrences Regulations
e-IRF	Electronic Incident Reporting Form
SI	Serious Incident
CCG/Collaboratives	Clinical Commissioning Group/Commissioning collaboratives
NRLS	National Reporting and Learning System
MHRA	Medicines and Healthcare Products Regulatory Agency
LRSAB	Leicestershire and Rutland Safeguarding Adults Board
LRSCP	Leicestershire and Rutland Safeguarding Children Partnership
QAC	Quality Assurance Committee
QF	Quality Forum
PSIG	Patient Safety Improvement Group
CPST	Corporate Patient Safety Team
DOLs	Deprivation of Liberty Safeguards
DOH	Department of Health
EHA	Environmental Health Agency
OLM	Organisational Learning Management database

1.0 Introduction

Leicestershire Partnership NHS Trust (LPT) The Trust is committed to supporting and embedding a positive reporting and learning culture within the organisation to enable the organisation to respond and learn where outcomes are not as expected or a near miss has been reported.

This policy describes the Trust's arrangements for reporting incidents of all types and of any significance and the actions expected to manage and follow-up such incidents. This policy also relates to any incidents involving staff, patients and others.

The collation and analysis of data on incidents and near misses is an intrinsic part of patient safety as it provides valuable opportunities to learn and improve.

LPT actively encourages the reporting of all types of incidents through electronic reporting and supports a 'just culture' in relation to such reporting.

Where staff do not feel able to report incidents they are encouraged to raise concerns through 'Freedom to Speak up Guardians' (FTSU) LPT are committed to learning from both the escalation and the reason for using the FTSU route.

To support our patients first 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 so that important lessons can be learned and acted on. This is undertaken on a background of openness and transparency, supporting patients, family and staff through the process.

2.0 Statement and Purpose of the Policy

2.1 This policy ensures that arrangements are in place to adhere to both the legislative and reporting requirements for NHS England/Improvement's current National Reporting and Learning System (NRLS) for incidents, Health and Safety Executive (HSE), Care Quality Commission (CQC) registration process, the Trusts commissioners and both internal and external stakeholders.

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

- Ensure a 'Just Culture' is developed, 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 Feb 2021.
- Ensure all appropriate levels of debrief and support to staff and the sharing of lessons learned takes place following incidents. See **Appendix 8** for guidance on staff using 'Debrief Flow Chart' following an incident for staff members and **Appendix 9** the 'Provision of Staff Welfare and Support Debrief Tool'

- Ensure all relevant internal and external Stakeholders, Agencies, and Regulatory bodies are engaged, involved and informed in line with National policy and guidance.
- Ensure lessons are learned from reported incidents, and take appropriate action to avoid a recurrence, including making changes to system, process, practice and/or the environment to improve patient and staff safety where appropriate.
- Ensure 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, disciplinary action which includes reporting to professional bodies will be considered.

The responsibilities of all staff for reporting, investigating and learning lessons from Serious Incidents (SI's) are set out in the Trust's Serious Incident Policy (incorporating Patient Safety Incident Investigations).

3.0 Executive Summary

This Policy describes the management of all incidents, clinical and non-clinical.

It outlines the responsibilities of all staff for reporting, escalating, investigating and learning lessons 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.

This policy applies to incidents on LPT premises, or on other premises where services are provided by LPT, or which occur as a direct consequence of LPT care.

Where an incident originates from outside of LPT the procedure is that the Corporate Patient Safety Team (CPST) will inform the Organisation to which the incident belongs. The CPST will via **ULYSSES** report such events (and tag as external).

The key requirements of this policy are:

- All incidents and near misses are reported in line with the timescales set out in local and corporate supporting 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 culture of fairness, openness and learning in LPT by making staff feel confident to speak up when things go wrong, rather than fearing blame.
- Supporting staff to be open about mistakes allows valuable lessons to be learnt 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.
- Incidents suspected of being Serious Incidents (SI) or 'Never Events' are escalated to the CPST as per 'LPT Serious Incident' policy.
- We investigate and learn from deaths as per the 'Learning from Deaths' policy.
- 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 February 2021.

- Application of other key policies which include LPT Adult Safeguarding and Children Safeguarding Policy 2019 and Allegations that an Employee/ Bank Worker may be Harming a Child, Young Person or an Adult at risk, Policy and Procedure (2018)
- That prompt investigation and intervention takes place to avoid recurrence.
- Feedback is provided and lessons learned are shared/action taken.
- Patients, staff and contractors who have been harmed receive appropriate support, explanation and apology.
- Any event recognised as an incident or SI retrospectively (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 to whom this evidence comes to light, and is subjected to appropriate investigation.
- There is timely review of harm, investigation and closure of incidents on the Ulysses system in line with timescales.
- Analysis of themes and trends take place, actions are agreed and implemented.

Please refer to section 7 (roles and responsibilities) for further detailed guidance.

4.0 Confidentiality application to Incident Reporting

Full names should only be recorded in the required section of the eIRF, not in the narrative/incident description. Investigation reports undertaken relating to an incident should contain anonymised information. Staff should be referred to by their job title where practical. Other individuals should be referred to by initials only.

5.0 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:

- 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 (known as 'near misses'). (NPSA, 2011)

6.0 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;

e.g. 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 period, or, as a result of a specific situation (hazard) e.g.:

- 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 a reportable incident. Where there is a mistake or an error involving a medication but there is no harm this is still a reportable incident. If a mistake or

error was intercepted so that it did not actually happen this would be a reportable near-miss from which learning must also be identified’.

Incident

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.

Serious Incident (SI) (SEE SI POLICY FOR INFORMATION REGARDING RESPONSIBILITIES AND PROCESS)

A Serious Incident is an accident or event in which:

- A patient, member of staff or member of the public suffers (or is exposed to the risk of) serious injury, moderate/semi-permanent harm, or unexpected death *or*,
- Actions of LPT staff are likely to cause significant public concern *or*,
- There might be serious impact upon the delivery of services and/or media attention and/or litigation and/or a serious breach of service standard or quality.

In addition, all ‘Never Events’ as defined by NHS England (2018) are Serious Incidents (including some moderate harm incidents). Please refer to the SI Policy.

Near Miss

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.
- A near miss is an incident that was prevented by chance rather than part of the process.

SEE APPENDIX 2 FOR EXAMPLES OF INCIDENTS

RIDDOR reportable Incident - SEE APPENDIX 3 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

6.1 Incidents that are linked to ‘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 commissioners must ensure that information about abuse or potential abuse is shared with Local Authority safeguarding teams.

Providers and commissioners must liaise regularly with the local authority 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 investigations are linked to patient safety investigations; services are to be guided by the CPST and Safeguarding

Child deaths (all subject to Child Death Overview Panel (CDOP)), significant harm and serious sexual abuse may or may not trigger an SI review; however all are reported to the Leicestershire and Rutland Safeguarding Children Partnership (LRSCP).

The interface between the serious incident process and local safeguarding procedures are articulated in the local multi-agency safeguarding protocol and policies and is further detailed in LPT's Serious Incident Reporting Policy.

Safeguarding Children and Child harm incidents

Where a child has been significantly harmed but not died as a result of an incident, the following considerations need to be explored as to whether the incident is an SI or not.

Has the harm occurred on NHS premises, as a result of NHS funded care, or caused by the direct actions of healthcare staff? If no to all the above, it's useful to consider whether or not the child has been in receipt of healthcare within the last 12 months. If so the case will need to be reported as an SI 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 declared an SI 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 recording on Ulysses.

Cases of death or significant harm, the case may also be investigated as a Serious Case Review under Safeguarding Adults procedures through the LRSAB. The interagency decision to investigate as a Safeguarding Adult Review (SAR) should not delay the investigation as an SI. The SI 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 untoward incident; however it does give a service an opportunity to review patient care and the intervention and should be considered for learning and not considered inevitable.

Such outcomes should be subject to Morbidity and Mortality Meeting review or a Modified Structured Judgement Case Review in the case of deaths (see "Learning from Deaths" Policy).

Directorates must ensure that an event recognised some time later as an incident or SI (in Mortality and Morbidity meetings or by other mechanism) is reported and is subjected to appropriate investigation. Where there is doubt about whether a SI or an incident has occurred, advice should be sought from a senior member of the Corporate Patient Safety Team.

6.2 Notifications of incidents involving patients/service users required to meet Health and Social Care Act 2008 requirements

The following incidents must be reported using the relevant Care Quality Commission (CQC) forms:

- Death of a detained (or liable to be detained) patient.
- Absence without leave of a detained (or liable to be detained) patient (occurring over midnight on any day).
- Applications to deprive a person of their liberty (DoLs).

These Notifications are required under the Health and Social Care Act 2008.

These notifications are undertaken in conjunction with the Lead Nurse for the service and the Quality & Compliance Team. Reference must always be made to the incident details and a copy where possible attached to the incident; if this is not possible the incident must be updated with this notification details.

Notification of Incidents in LPT

All incidents are reported via an electronic incident database called '**Ulysses**'. This allows staff to easily report all incidents and for Trust teams to collate incident information for local and national reporting. Staff are encouraged to report incidents locally and LPT aim's to provide an open and just culture to support this. However should staff feel unable for whatever reason they are also able to raise concerns through 'Freedom to Speak up Guardians' as part of the Trust's 'Freedom to Speak Up: Raising Concerns (Whistleblowing) Policy.

7.0 Roles and Responsibilities

Whole Trust

LPT has an ethical obligation to patients who use our services and to provide staff with a mechanism to report staff/organisational incidents and a legal obligation to ensure that all incidents, accidents and near misses are managed, reported and actioned appropriately. We are accountable to our commissioners, through contracting and commissioning arrangements, NHS England, Care Quality Commission and Information Commissioners Office, Public Health England and Health and Safety Executive. This list is not exhaustive.

The Trust recognises its role and responsibility to external regulatory and monitoring agencies, and other external stakeholders. [SEE APPENDIX 1.](#)

Key duties

Chief Executive will have:

- 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 Assurance Committee (QAC) 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.

All Directors will within their own areas of responsibility

- Ensure that internal and external reporting requirements are met.
- Ensure that 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 care pathways and that assurance and monitoring takes place.
- Ensure that their service care pathway 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 investigation findings and learning.

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 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 Governance Teams

- In liaison with the Corporate Patient Safety Team (CPST) provide quality assurance of the reporting and the grading of 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 and Incident Oversight Group.
- Work with and support the local teams and the Corporate Patient Safety Team to ensure the timely management of incidents, providing incident information as required.
- Work in liaison with Directorate Teams/Matrons 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 should be stored within Ulysses to ensure there is a central repository of all relevant information. This includes investigation records & 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 as detailed in section 2.2 of the policy

Specialist staff

- Advise and assist in the reporting, investigation and the timely action of incidents relevant to their role. **Specialist staff can include;** the Health and Safety Advisors, Patient Safety Manager, Manual Handling Lead, Infection Prevention & Control Lead, Safeguarding Lead, Fire Officer, Security Management Advisor, Emergency Planning Lead etc.

Medical Director

- 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 staff with Leadership and Management Responsibility

- To ensure that all incidents are correctly categorised, the level of harm is accurate and appropriate action has been taken to both ensure the patient or member of staff is safe and escalate or act as part of the closure of all incidents. This information needs to be recorded on Ulysses.
- Ensure that they, and the staff they are responsible for complying with and supporting the implementation of this policy.
- Ensure that all staff can access training in the form of local induction covering incident reporting and support further training identified in relation to incident management, investigation and learning according to their roles.
- Ensure staff report all incidents effectively and where necessary, local investigations are undertaken and learning identified and implemented.
- Consider and use incident data in risk assessments as appropriate as part of complying with the Risk Register process.
- Escalate concerns and incidents that may meet the threshold for Serious Incidents.
- Take action to mitigate against recurrence and to provide feedback and learning through their local forums, which must form part of their incident evidence.
- Review the Grade of incidents and approve them before closure submission to the incident management database, Ulysses.
- Undertake, participate themselves and ensure staff participation in any local incident investigation
- Support staff involved in and/or affected by an incident in line.
- Ensure that lessons learned are fed into local forums. Review trends on a regular basis and where necessary, develop action plans to reduce likelihood.
- Ensure a regular reporting mechanism exists with line manager, Matron, Deputy Heads of Nursing or Head of Service/Nursing.
- Ensure that incidents are investigated and closed in a timely way; this should be within 15 working days of the incident being reported. It is expected that a majority will be investigated and closed within 10 working days with the exception of incidents that are deemed a 'Serious Incident'. [\(SEE APPENDIX 4 FOR GRADING AND TIMESCALES\)](#)
- All teams that are involved in managing incidents must ensure they are appropriately categorised and all records related to incidents are stored only in Ulysses. No local electronic files related to incidents will be kept. **H & S /RIDDOR information is stored on other files and provide the information as requested.**

The Corporate Patient Safety Team (CPST) will ensure that:

- Incidents are 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 directorate and departments via Trust Committees, education and training programmes, websites, newsletters and bulletins and support given as requested to undertake this at local directorate level.
- In conjunction and when requested by the Directorate Governance Teams; ensure information and training is provided for staff regarding reporting, grading and investigation of incidents and completion of eIRFs. Additional support will be provided for the clinical leadership teams to ensure triage of incidents is timely and escalation of incidents is undertaken as required.

ALL Employees are required to:

- 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.
- Not to 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
- Comply with the requirements of 'Being Open Policy/Culture of candour' in relation to incidents in communicating incident information to those affected.
- Participate in investigation and implementation of learning from incidents.
- Act on and report in accordance with this policy any incident that is brought to their attention by a patient, visitor or contractor and colleague.

8.0 Quality checking

All staff who access the Ulysses incident record, have the responsibility to quality check the recorded details to ensure all relevant fields are completed and in line with the incident description, lessons learnt have been recorded and redact patient or staff identifiers within the description to avoid Information Governance breaches.

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. 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. This is facilitated by CPST.

8.1 Reporting to the National Reporting Learning System (NRLS) the current NHS wide learning database for patient Safety incidents (this is planned to change 2020/21)

All Patient Safety Incidents (PSI) must be uploaded by the Incident Administration Team Members of the CPST to the National Reporting Learning System (NRLS) within their agreed monthly timescales. Locally our standard is that this is undertaken weekly.

8.2 Incident Reporting Process

Immediate Action Following the recognition that an Incident has occurred

Identifying an incident or near miss is the first stage of risk management. Immediate action to be taken following an incident is described below.

Any member of staff present when an incident is discovered must take immediate action to reduce further risk and in maintaining safety, ensure that their own safety is not compromised.

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 in the designated area.

The following factors should be taken into account in order to determine the necessary escalation:

- The extent of harm caused and the immediate first aid and support needed to the injured or traumatised
- 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 and those involved, including staff, in the incident should be supported and given an explanation of the incident, its consequences as far as is known and the treatment available and what immediate actions are necessary to minimise further risk or injury. This communication should take place as soon as possible.
- 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 important responsibility.
- Nurse Associate/Support Workers must escalate the incident to their line manager; RN/AHP. **It is the responsibility of the RN/AHP 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 important responsibility.
- RNs / AHP's in charge of shifts/Teams/Mental Health Clinical Duty 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 important responsibility.**
- **Currently, Band 6 and above RNs / AHP's /Mental Health Clinical Duty Managers are responsible for updating the incident report regarding the outcome;** 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

- Every incident must be reported on the Trust's Electronic Incident Report Forms by way of Ulysses Database. Incidents should be reported within 24 hours of becoming aware of the event. This includes all types and grades of incidents. All sections of the form should be completed covering immediate post-incident actions and is accessed via the Trust' intranet page.
- An event may only be recognised as an incident sometime after the event; in such cases the member of staff to whom such evidence comes to light must report the incident as described in this policy. The passage of time is not a reason not to report.
- Incidents and near misses should be reported on Ulysses as close to the time of the incident as practicably possible. To support the interrogation of trends and themes the reporter is required to allocate the incident a cause groups/types (also known as a category and sub-category). As 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 report should be free from jargon, personal 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.

This guidance is for all staff. It also relates to any manager taking responsibility for the local investigation of an incident

Immediate Management of the Incident and communications

- The senior member of staff in charge of the service area 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 the next of kin have been contacted, where necessary, and an incident form has been correctly completed so that reporting to senior managers and Directors can take place if appropriate; this is known as 'Heads Up' when it is submitted.
- The most senior member of staff has the responsibility of verbally reporting incidents that have the potential to be a 'serious incident' (SI) via the management structures

Supporting staff

The manager of the area will ensure that those involved in or 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.

Where an incident of assault to a member of staff has occurred and is reported, an alert is automatically sent as a notification to the Security Management Advisor.

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 who are responsible for reporting to the HSE without delay. [SEE APPENDIX 3 FOR INFORMATION](#)
- If a member of staff is involved they are provided with appropriate support including a referral to Occupational Health Department or Emergency Department if injured and where this is deemed necessary.
- CPST, in conjunction with Line Managers/Deputy Heads of Nursing/Heads of Nursing/Services will ensure that **any Initial Service Managers Reports/72hr reports** are requested for all incidents that may require higher level of investigation. Directorate Governance Teams are responsible for ensuring completion and return to the CPST within the timescale and that local clinical oversight has taken place in readiness for review at the weekly Incident Review Forum. This is paramount for timely sharing with CCG, CQC and informing patients/families of next steps.

Head of Trust Health and Safety Compliance in the event of an incident that is: reportable under RIDDOR or has resulted in 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. [\(SEE APPENDIX 3 FOR MORE INFORMATION\).](#)

The Head of Trust Health & Safety Compliance will be responsible for:

- Assessing the level of investigation required;
- Undertake as appropriate RIDDOR reporting and incident investigation.
- To liaise with the Health & Safety Executive as required

- **Head of Data Privacy /Data Protection Team**

In the event of an incident involving security of information the Information Governance/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.

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 Patient Safety Team, 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.

The Guidance for process and assessment of the severity of the incident can be found in the [APPENDIX 6](#).

The immediate response to an information breach incident and the escalation process for reporting and investigating will vary according to the severity of the incident.

9.0 Managing Incidents

- Reviewing Incidents for appropriate investigation –

The Directorate local ward/department manager, senior nursing and team leads in conjunction Directorate Governance Teams are responsible for reviewing and identifying appropriate level of investigation. CPST also undertake the triage role to support timely escalation/investigation.

Incidents that are considered to potentially require further review for level of investigation will be reviewed through the **Incident Review Meeting (IRM)** Process on a weekly basis. This process involves members of the CPST, senior nurses and members of the directorate governance teams. There is an expectation that senior nurses responsible for the area where the incident has occurred will have undertaken the initial review and present the findings to the group. There will be some of these incidents that may meet the serious incident (SI) criteria either due to the national framework or the great opportunity for learning and supporting change.

For incidents that have been declared an SI please refer to the Trust Serious Incident Policy.

Advice/support is available from the CPST and Directorate Governance Teams on all aspects of this policy and supporting procedures, including 'writing an account of events' (factual account template – see [Appendix 7](#)), conducting and organising interviews/round tables, and investigation processes.

9.1 Being Open and the statutory Duty of Candour

The Trust seeks to promote a culture of openness, which is a pre-requisite for improving patient safety and the quality of healthcare systems.

CQC Regulation 20 states that a 'Health Service body must act in an open and transparent way with relevant persons in relation to care and treatment provided to services users in carrying on a regulated activity'.

Patients, Families/carers (relevant person) they must be fully informed of the facts and offered an apology and appropriate support. An account should be provided of all the facts the Trust knows about the incident as at the date of the notification and any further facts as they arise.

The Trust should make every reasonable effort to contact the relevant person through various communication means, if the relevant person declines to contact the provider, their wishes should be respected and a record of this kept.

There may be rare occasions where it may not be appropriate to contact the relevant persons, for example during a Police investigation of an incident – advice should then be sought from the CPST.

The detail of the discussion must be recorded in the patient's medical records and the incident report form on Ulysses so that subsequent staff are aware and for audit purposes.

The Trust must keep a copy of all correspondence along with timelines with regards to the notification to the 'relevant person' on Ulysses; **local files must not be created.(NB only with extreme sensitivity and then a file note should be made & advice sought from data privacy team if unsure). RIDDOR/Health & Safety – as before have their own system for storage.**

9.2 Incident Investigation, action planning, managing and closure

High incident reporting organisations are on the whole safer ones, with a more effective safety culture; in which the severity of incidents frequently falls as the number (and learning) increases.

Incident management can help ensure that resources are targeted effectively when implementing solutions to prevent a recurrence and can provide an early warning of potential complaint or litigation.

The comprehensive management of incidents allows prompt action to be taken to minimise the effects of the incident, reduce risk and improve safety of patients, staff and visitors. A proactive approach to safety enhances the Trust's reputation and public confidence

Incident investigation should take a structured approach seeking to describe all the contributory factor(s) to an incident. Together with consideration of the wider system through an appreciation of human factors and ergonomics, this approach enables the development of comprehensive solutions to reduce risks.

An incident rarely arises because of a single event. The causes are generally multiple and often extend beyond one individual. Several factors influence the degree of investigation required:

- The seriousness of the event, including degree of harm suffered effects on service delivery, reputation of the Trust.
- The likelihood of recurrence.
- The potential for learning and changing practice.
- Frequently occurring incidents even when no harm is caused.

All incidents are graded according to degree of actual harm.

[APPENDIX 4](#) describes the current guide around the level of investigation required, timescales for investigating and closure. For further information regarding serious incident investigation timescales and levels of harm staff should refer to the 'Serious Incident policy'.

The comprehensive management of incidents allows prompt action to be taken to minimise the effects of the incident, reduce risk and improve safety of patients, staff and visitors. A proactive approach to safety enhances the Trust's reputation and public confidence.

It is good practice (and recommended) that staff involved in an incident write their own personal account of events as soon as possible and while memories are fresh. These will support individual staff should they be required to provide a written account of events as part of the investigation process.

[SEE APPENDIX 7](#) for a 'Factual account templates' that assists in the investigation process; further help can be sought from CPST.

9.3 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.

10.0 Information Technology (IT) Incidents

[PLEASE SEE APPENDIX 5](#) for a guide to the management of IT incidents within LPT.

The immediate response to the incident and the escalation process for reporting and investigating will vary according to the severity of the incident.

11.0 Information Governance /Data Privacy Incidents and Assessing Severity – the Trust has to comply with the Information Commissioners Office with matter of information breaches. [PLEASE SEE APPENDIX 6 FOR DETAIL](#)

□ Assessing the severity of the incident

The immediate response to the incident and the escalation process for reporting and investigating will vary according to the severity of the incident. The Information Governance Team should be contacted to determine the level and severity of the incident using the national incident grading system.

□ Informing Patients

It is good practice to consider informing patients when person identifiable information about them has been lost or inappropriately placed in the public domain. Where there is any risk of identity theft it is strongly recommended that this is done.

12.0 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, the incident may have occurred in 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.

Where an incident is discovered which may have originated in another organisation who were involved in the care of the patient, the CPST should be contacted so that the appropriate stakeholders can be informed and involved in the investigation.

13.0 Healthcare Associated Infections Infection prevention and control incidents

Staff must report all incidents pertaining to infection prevention and control in accordance with LPT reporting procedures. This will include non-adherence with infection prevention and control procedures. Habitual non-adherence to the policy may result in disciplinary action being taken. Root cause analysis will be used to investigate serious incidents to determine system failure or care delivery problems.

Criteria for defining an infection 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*
- Death associated with MRSA
- Bowel surgery associated with *Clostridium difficile*
- MRSA Bacteraemia
- Water management issues
- Legionella
- Sharps injuries
- Covid19

An incident report form must be completed for each of the above. This automatically alerts the Infection Prevention & Control Team (IPCT) who will take appropriate action. Any additional information can be obtained directly from the IPCT.

Serious Incident report (SI)/Root Cause Analysis (RCA) should be commenced for the following identified as community acquired infections:

- 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
- Severe harm or death as a result of a hospital acquired infection (inc COVID)

14.0 Screening Incidents

National screening programmes are public health interventions, which aim to identify disease or conditions in defined populations in order 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. These incidents are reported via Ulysses and then directly reported to Specialist Commissioners for Screening following a specific investigation pathway which the CPST will facilitate.

15.0 Pressure Ulcers/Tissue Viability

All pressure ulcers that are identified during LPT care contact must be reported through the incident reporting process whether they 'developed during our care or were present on admission'.

16.0 Inpatient Falls

All inpatient falls that occur or are identified during LPT care must be reported through the incident reporting process. All falls with harm that result in fracture or death of a patient in LPT are currently escalated for investigation as a SI due to the level of harm and distress to the patient and their families. It is essential that staff go back in and update the incident if the harm is identified at a later date and escalate to the CPST

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 being open with patients/families should not be delayed as a result of an interruption to the system.

To summarise

As part of the Trust's commitment to keep patients and staff safe it is required to have a robust incident reporting system and processes to support the identification, reporting, investigation, escalation as required and learning from incidents locally and across the healthcare community. It allows for identification 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.

APPENDIX 1 – EXTERNAL STAKEHOLDERS

Area of concern	Responsible Body	Reporting Responsibility
Serious Incident	Relevant Commissioners	Head of Patient Safety /Patient Safety Manager
Most Serious Events including Never Events	Relevant Commissioners, CQC, NHSE/I	Head of Patient Safety /Patient Safety Manager
Request to conduct incident investigation	Healthcare Safety Investigation Branch (HSIB)	Head of Patient Safety
Medical Devices	Medicines and Healthcare Products Regulatory Agency (MHRA)	Medical Devices Lead/Medical Devices Safety Officer, Head of Patients Safety Lead
Medicines	MHRA Safety alerts	Medicines safety officer/chief pharmacist
Reporting of Injuries, Diseases and Dangerous Occurrences (RIDDOR)	Health and Safety Executive	Head of Health and Safety Compliance
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	Head of Patient safety, Patient Safety Manager and Responsible Director
Media interest	The Media	Communications Lead and Chief Executive
Medication issues	Medicines and Healthcare Products Regulatory Agency (MHRA)	Pharmacy Lead
NHS Safety alerts	NHS Central Alert System	Risk & Assurance Lead, Head of Patient Safety
Criminal matters	Police	Head of Patient Safety Security Management Advisors
Fire related issues	Leicestershire Fire and Rescue	Head of Health & safety Compliance. Fire Officer/ Health & Safety Advisors.
Safeguarding	Leicestershire County Council/ CCG	Safeguarding Lead Practitioners
Estates and Facilities	NHS Estates & safety	General Manager – Facilities
Environment Agency		
Copies of independent investigation reports by external agency	Care Quality Commission	Executive Director of Nursing/AHP's /Chief Executive
Audit information on suicides and homicides	National Confidential Enquiry into Suicide and Homicide by People with Mental Illness	Suicide Prevention Lead Safeguarding team

Security incidents (fraud)	NHS Counter Fraud Service (CEAC)	Security Management Advisor
Unexpected death of patients under a section of the Mental Health Act 1983	The Trust Act Commission (now the Care Quality Commission)	The Trust Mental Health Act Manager/ Head of Patient Safety or Deputy Head of Patient Safety
General Medical Council	Concerns in relation to medical staff practice/conduct	The Medical Director
Nursing and Midwifery Council	Concerns in relation to nursing staff practice / conduct	Executive Director of Nursing and Quality/AHP's or delegated deputy
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

APPENDIX 2: EXAMPLES OF INCIDENTS

- Please note that this is not an exhaustive list but merely an indication of the types of incidents that should be routinely reported:
- 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, IV 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; 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.
- 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.
- Ongoing faults that successive service/maintenance visits have failed to rectify

APPENDIX 3: 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 onto LPT incident reporting system 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 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.
Retain RIDDOR reports for minimum of 10 years.
- Please contact the Health, Safety and Compliance Team for further information.

APPENDIX 4: SEVERITY GRADING AND TIMESCALES FOR CLOSURE

All incidents are graded according to degree of avoidable harm and the table below describes the level of investigation required and the timescales for completion the NHS (SI Framework, 2015); however, following the NHSE/I Patient Safety Strategy 2019 this is likely to alter with the further involvement of patients, families and teams by agreeing individual SI investigation timescales. For further information regarding incident investigation timescales and levels of harm staff should refer to the Serious Incident policy and the Corporate Patient Safety Team.

****	Severity Classification	Level of investigation required	Timescale for completion	Submitted to or part of reports
1	No harm	At the Manager's discretion	15 working days	Local / Specialty Clinical Governance Forum
2	Low harm	Local investigation by the Manager or appointed deputy	15 working days	Local / Specialty Governance Forum
3	Moderate harm that does not meet SI Criteria	Local 'Internal' investigation by the Manager or appointed deputy – with senior manager involvement** exception ** see Serious Incident policy for definitions of specific categories designated as SIs	30 working days	Incident Review Forum via 72hr Report and Local Speciality / Directorate Governance Forum.
4	Moderate/Severe harm	SI investigation - in accordance with the current NHS SI Framework (2015)	60 working days	Incident Review Forum via 72hr Report and Local Speciality / Directorate Governance Forum, CCG, CQC.
5	Death caused by incident	SI investigation - in accordance with the current NHS SI Framework (2015)	60 working days	As above - Claims and Inquest, Learning from Deaths Group, CCG, CQC
6	Complex incidents that meets SI Criteria that are so serious of wider learning than LPT	Current NHS SI Framework (2015) describes Level 3 external investigations (to NHS Trust by independent investigator) Healthcare Safety Investigation Bureau (HSIB)	Up to 6 months from commissioning external investigation however, this can be longer and is managed in conjunction with investigation body and CPST	Incident Review Forum Local Speciality / Directorate Governance Forum via 72hr Report PSIG. Management Board CQC CCG
7	Information/Data Breach	All are assessed to see if the incidents meet trigger for submission of information to Information Commissioners Office within 72hrs. Information to be supplied in 48hrs.	Individually led according criteria of investigation met	48hr Data Breach initial Review to data Privacy team Incident Review Forum Local Speciality / Directorate Governance Forum ICO, CCG

APPENDIX 5: INFORMATION TECHNOLOGY (IT) INCIDENT MANAGEMENT GUIDANCE

User /Service identify actual / potential clinical Incident involving IT (impact on services & delivery of care)

↓
First action must be to report via 'HIS Service Desk'

Does it involve a 'NATIONAL PROGRAMME FOR IT'? e.g. SystemOne i.e. potential to affect many patients/staff from undertaking their role



YES

NO

Local Service Desk (HIS) informed by telephone as urgent request

Local incident reporting mechanisms initiated as per local procedures e.g. Incident reporting via eIRF



Escalation by Senior IT Manager to Trust Team to take view as to whether incident escalated to NHSE/ NHS Digital



IM & T Lead Director to escalate to NHSE / NHS Digital & designate liaison with CCG



Consideration must be given by IM & IT lead for the involvement of the **NHS Digital Clinical Safety Officer (CSO)** with any complex IT Outage involving clinical IT applications



NHS Digital Clinical Safety Officer (CSO) to provide review and report support to Trust

APPENDIX 6: GUIDE TO THE NOTIFICATION OF DATA SECURITY AND PROTECTION INCIDENTS. (DEPARTMENT 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.

Impact	Catastrophic	5	5	10	15 20 25 Reportable to the ICO DHSC Notified		
	Serious	4	4 No Impact has occurred	8 An impact is unlikely	12 16 20		
	Adverse	3	3	6	9 12 15 Reportable to the ICO		
	Minor	2	2	4	6 8 10		
	No Impact	1	1 2 No Impact has occurred 3 4 5				
			1	2	3	4	5
			Not Occurred	Not Likely	Likely	Highly Likely	Occurred
			Likelihood harm has occurred				

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:

- (a) The alleged commission of offences by the data subject **or**
- (b) 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?

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 2020)

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?

Summary Notes

Please read and delete the guidance notes *written in blue in the right hand column before inserting your own entries*

Please remember; submission of summary notes or a statement is not about blaming you or others. ‘The purpose of an investigation is to understand how things usually go right as a basis for explaining how things occasionally go wrong’ (Hollnagel 2015)

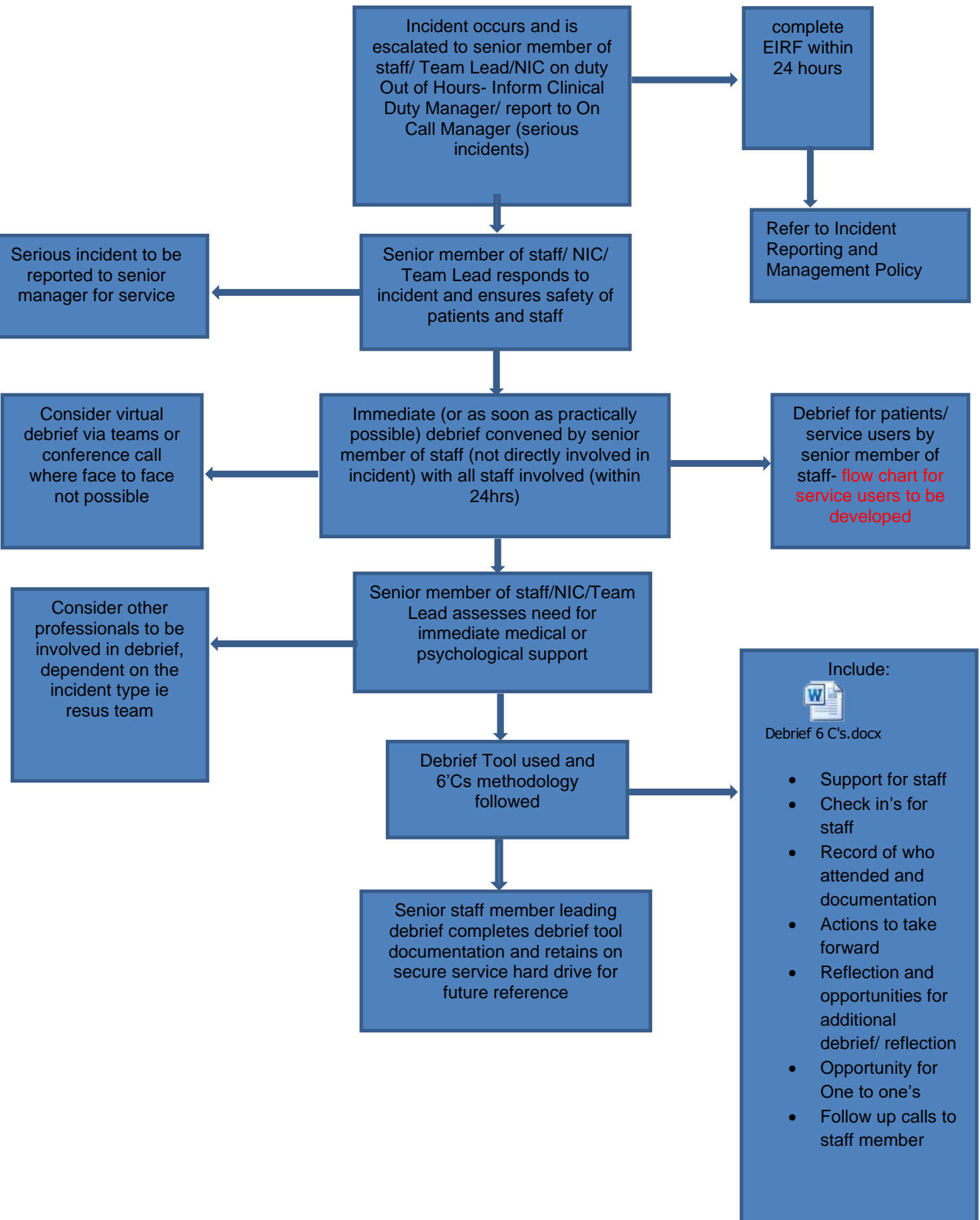
Name	<i>e.g. Mary Smith</i>
Position & role during the event reported	<i>e.g. RGN/HCA</i>
Qualifications	<i>e.g. Diploma in Nursing</i>
PIN/GMC Number	
Experience	<i>I qualified as a in 2002 and have worked in this dept. /ward</i>
Date/Time of Incident	<i>e.g. 6 September 2016 – 14.30 Hours (use 24-hour clock)</i>
Ulysses Nos	
Location	<i>e.g. Coalville Hospital ward..... (be as precise as possible)</i>
Factual Account	<p>Your Summary Notes should:</p> <ul style="list-style-type: none"> • <i>Consist of a complete factual account with sequential dates, times and venues.</i> • <i>Be clear and concise.</i> • <i>Refer not only to what is recorded in the notes but also to any other detail that can be recalled. If you cannot remember, do not make it up</i> • <i>Explain where the notes have been relied upon in their entirety by using the phrase ‘According to the notes...’</i> • <i>Be concerned only with what you actually did and why.</i> • <i>Anticipate any questions and provide responses.</i> • <i>Comment on any criticisms and your involvement.</i> • <i>Include any mitigating circumstances if an error has been identified.</i> • <i>Include any relevant conversations using direct speech and inverted commas, e.g. Dr X said ‘I will return in...’</i> • <i>List the full names of any other staff involved or present.</i> • <i>Where possible, be typed as statements are often photocopied.</i>

	<p>Your Summary Notes <i>should not:</i></p> <ul style="list-style-type: none"> • <i>Be a simple regurgitation of written case notes.</i> • <i>Comment on areas outside of your responsibility.</i> • <i>Include irrelevant, subjective comments about the patient or colleagues</i> • <i>Include abbreviations or clinical terminology - It should be written in a way that is understandable to a layperson.</i> • <i>Include statements that cannot be proven, e.g. 'I think he was drunk', without qualification, e.g. 'because he smelt strongly of alcohol.'</i> • <i>Contain words you do not understand.</i>
Professional Reflection	<ul style="list-style-type: none"> • <i>What sort of day/shift were you having? Did this influence what is reported to have happened?</i> • <i>Would you do anything differently in the future if faced with the same clinical scenario?</i> • <i>Would you like further support?</i>
What went well	<ul style="list-style-type: none"> • <i>It is important what you consider went well during the delivery of patient care i.e. teamwork, knowledge & skills of self or others</i>
Were there any exceptions (+ve & -ve) to the usual processes for caring for this type of patient?	<ul style="list-style-type: none"> • <i>i.e. theatre team you worked with, availability of resources</i>
Statement of Truth	I believe the contents of these summary notes to be true.
Signed	
Print	
Date	
Address	Leicester Partnership NHS Trust

Retain a copy of this document in a secure place as part of the incident record

A copy of this document **must not** be filed in the patient's healthcare record

APPENDIX 8: Debrief Flow Chart following an incident- Staff Members





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
<p>1. Care <i>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.</i></p>	<ul style="list-style-type: none"> • How is everyone feeling? (physically/emotionally?) • What did that experience feel like? • What do you think will help you now? 	
<p>2. Compassion <i>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</i></p>	<ul style="list-style-type: none"> • 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? 	

	Discussion Points	Notes and Actions
<i>people perceive their care.</i>		
3. Competence <i>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.</i>	<ul style="list-style-type: none"> • 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 <i>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 our care and staff alike.</i>	<ul style="list-style-type: none"> • 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? 	
5. Courage <i>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.</i>	<ul style="list-style-type: none"> • 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 <i>A commitment to our</i>	<ul style="list-style-type: none"> • Reflecting on the incident, is there anything that you think 	

	Discussion Points	Notes and Actions
<i>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.</i>	<ul style="list-style-type: none"> • could have been done differently? • our learning points? • we need to do to prevent or manage these types of incidents in the future? 	<p style="text-align: right;">What are</p> <p style="text-align: right;">What do</p>

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 10: DUE REGARD SCREENING TEMPLATE

Section 1			
Name of activity/proposal		Incident Reporting Policy	
Date Screening commenced		June 2021	
Directorate / Service carrying out the Assessment		Corporate Patient Safety Team	
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:			
<p>AIMS: To establish a clear and consistent approach to the reporting, investigation and management of incidents.</p>			
<p>OBJECTIVES: To provide a safe environment for patients, staff and visitors.</p>			
Section 2			
Protected Characteristic		If the proposal/s have a positive or negative impact please give brief details	
Age		It has neutral impact on all the protected characteristics.	
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.			
Yes		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:			
Discussion at PSG			
Signed by reviewer/assessor		S Arnold	Date 20/06/2021
Sign off that this proposal is low risk and does not require a full Equality Analysis			
Head of Service Signed			Date 21/06/2021

APPENDIX 11: TRAINING NEEDS ANALYSIS

Training Required	YES ✓	NO
Training topic:	Incident Reporting and Management of Incidents	
Type of training: (see study leave policy)	<input type="checkbox"/> Mandatory (must be on mandatory training register) <input checked="" type="checkbox"/> Role specific <input type="checkbox"/> Personal development	
Directorate(s) to which the training is applicable:	<input checked="" type="checkbox"/> Mental Health <input checked="" type="checkbox"/> Community Health Services <input checked="" type="checkbox"/> Enabling Services <input checked="" type="checkbox"/> Families Young People Children & Learning Disability Services <input checked="" type="checkbox"/> Hosted Services <input checked="" type="checkbox"/> Corporate Teams	
Staff groups who require the training:	All Staff groups-Incident reporting Band 7 and above-Investigator/handler of incidents	
Regularity of Update	3 years or as changes occur with incident reporting or systems used to manage incidents	
Who is responsible for delivery of this training?	Corporate Patient Safety Team, Local Directorate Governance Teams & Local Services	
Have resources been identified?	Yes	
Has a training plan been agreed?	Yes	
Where will completion of this training be recorded?	<input checked="" type="checkbox"/> ULearn <input type="checkbox"/> Other (please	

	specify) – face to face group/Virtual and individual as required
How is this training going to be monitored?	Evaluation

APPENDIX 12: 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	<input type="checkbox"/> X
Respond to different needs of different sectors of the population	<input type="checkbox"/> X
Work continuously to improve quality services and to minimise errors	<input type="checkbox"/> X
Support and value its staff	<input type="checkbox"/> X
Work together with others to ensure a seamless service for patients	<input type="checkbox"/> X
Help keep people healthy and work to reduce health inequalities	<input type="checkbox"/> X
Respect the confidentiality of individual patients and provide open access to information about services, treatment and performance	<input type="checkbox"/> X

Key individuals involved in developing the document

Name	Designation
Susan Arnold	Corporate Patient Safety Lead Nurse - CPST
Tracy Ward	Head of Patient Safety
Jo Nicholls	Patient Safety Manager – CPST
David Adamson	Incidents Administration Support - CPST

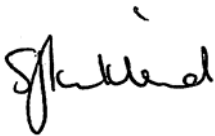
Circulated to the following individuals for comment

Name	Designation
PSIG Group email	Correct as of October 2020
Sam Kirkland	Head of Data Privacy/Data Protection Officer
Trust Health & Safety Team	Trust Specialist Leads for Health and Safety
Ian Wakeford	Trust Lead Head of Trust Informatics (for Information Technology)
Anne Scott	Director of Nursing & Allied Health Professionals
Deanne Rennie	Deputy Director of Nursing & Allied Health Professionals
CPST	Corporate Patient Safety Team Members
Alison Taylor-Prow	Lead Nurse for safeguarding Adults
Dean Cessford	Senior safeguarding Practitioner
Amanda Hemsley	Lead Infection Prevention and Control Nurse
Antonia Garcia	Senior Infection Prevention and Control Nurse
Charlotte Harris	DMH Governance Administration Support
Rachel Shaw	DMH
Rachel Travis-Pruden	Deputy Head of Nursing – DMH
Alison Kirk & Matthew Smith	Reps for Patient Experience Team
Simone Logue	Safeguarding Practitioner
Ann Jackson	Lead Nurse for Suicide Prevention
Michelle Churchard	Head of Nursing DMH
Louise Evans	Deputy Head of Nursing FYPC
Sarah Latham	Deputy Head of Nursing CHS
Tracy Yole	Matron
Jane Martin	Matron
Kerry O'Reardon	SI Lead DMH
Neil King	Head of Safeguarding
Lyn Williams	Assistant Director of Quality Improvement
Helen Walton	Lead for LPT estates
Kathryn Price	FYPC Governance Administration Support
Jude Smith	Head of Nursing CHS
Rachel Tolley	Acting Lead for Governance FYPC

Appendix 14 Data Privacy Impact Assessment Screening

DATA PRIVACY IMPACT ASSESSMENT SCREENING

<p>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.</p> <p>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.</p>		
Name of Document:	Incident Reporting Policy	
Completed by:	Sue Arnold	
Job title	Corporate Patient Safety Team/Interim Patient Safety Incident Investigation Lead (DMH)	Date 15th December 2021
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?	Yes	Information could be shared with individuals within LPT for the purpose of understanding themes but no patient identification details.
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.	Yes	Any email correspondence is secure and anonymised.
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 privacy concerns or expectations? For examples, health records, criminal records or other information that people would consider to be particularly private.	Yes	Patient information will shared in a secure database to record incidents,
8. Will the process require you to contact individuals in ways which they may find intrusive?	No	
<p>If the answer to any of these questions is 'Yes' please contact the Data Privacy Team via Lpt.dataprivacy@nhs.net</p> <p>In this case, ratification of a procedural document will not take place until review by the Head of Data Privacy.</p>		

Data Privacy approval name:	Sam Kirkland, Head of Data Privacy 
Date of approval	17.12.2021

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

Data Privacy Impact Screening Guidance Notes

The following guidance notes should provide an explanation of the context for the screening questions and therefore assist you in determining your responses.

Question 1: Some policies will support underpinning processes and procedures. This question asks the policy author to consider whether through the implementation of the policy/procedure, will introduce the need to collect information that would not have previously been collected.

Question 2: This question asks the policy author if as part of the implementation of the policy/procedure, the process involves service users/staff providing information about them, over and above what we would normally collect

Question 3: This questions asks the policy author if the process or procedure underpinning the policy includes the need to share information with other organisations or groups of staff, who would not previously have received or had access to this information.

Question 4: This question asks the author to consider whether the underpinning processes and procedures involve using information that is collected and used, in ways that changes the purpose for the collection e.g. not for direct care purposes, but for research or planning

Question 5: This question asks the author to consider whether the underpinning processes or procedures involve the use of technology to either collect or use the information. This does not need to be a new technology, but whether a particular technology is being used to process the information e.g. use of email for communicating with service users as a primary means of contact

Question 6: This question asks the author to consider whether any underpinning processes or procedures outlined in the document support a decision making process that may lead to certain actions being taken in relation to the service user/staff member, which may have a significant privacy impact on them

Question 7: This question asks the author to consider whether any of the underpinning processes set out how information about service users/staff members may intrude on their privacy rights e.g. does the process involve the using specific types of special category data (previously known as sensitive personal data)

Question 8: This question asks the author to consider whether any part of the underpinning process(es) involves the need to contact service users/staff in ways that they may find intrusive e.g. using an application based communication such as WhatsApp

If you have any further questions about how to answer any specific questions on the screening tool, please contact the Data Privacy Team via lpt.dataprivacy@nhs.net

APPENDIX 15: REFERENCES AND BIBLIOGRAPHY

THE POLICY WAS PREPARED WITH REFERENCE TO OR /REVIEW OF THE FOLLOWING DOCUMENTATION/WEBSITE REVIEW:

<https://improvement.nhs.uk/resources/patient-safety-strategy/>

<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/documents/5114/Guidance_for_reporting_pressure_ulcers.pdf (2018)

https://improvement.nhs.uk/documents/2932/NSTPP_summary__recommendations_2.pdf (2018)

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

Freedom to Speak Up: Raising Concerns (Whistleblowing) Policy. (2019)

LPT A Culture of Candour Policy (Incorporating 'Being Open' and 'Duty of Candour) February 2021.

LPT 'Adult Safeguarding' and 'Children Safeguarding' Policy 2019 (separate policies)

LPT 'Allegations that an Employee/ Bank Worker may be Harming a Child, Young Person or an Adult at risk', Policy and Procedure (2018)

LPT Infection Prevention and Control Overarching Policy (2018)

Incident Reporting Policy and Procedure Lincolnshire Community Health Services NHS Trust (2018)

Northamptonshire NHS Foundation Trust Incident Reporting Policy (2020)

Nottingham University Hospitals Incident Reporting Policy (2018)

Sherwood Forest Hospitals Incident Reporting Policy (2019)