The Tavistock and Portman
NHS Foundation Trust

Incident Reporting Procedure

Type	Corporate
Version:	10.1
Bodies consulted:	EMT
Approved by:	EMT
Date Approved:	7 December 2021
Lead Manager:	Health and Safety Manager
Responsible Director:	Medical Director
Date issued:	December 2021
Reviewed date:	October 2024
Intranet?	YES
Extranet?	NO

Audit trail –

Version	Amendments	Name & Date
V10 June 2019	Updated to include implementation of new QP electronic Incident reporting System, and the procedures in submitting an Incident report. Removed all flow charts and RIDDOR appendices 'Serious incident' and 'Reportable disease' definitions updated Introduced the Incident panel Reviewed and updated roles and responsibilities	Lisa J Tucker Health and Safety Manager
June 2020	Reviewed and updated workstream reporting to the Integrated Governance Committee. The dissolution of the CGR workstream and submitting the risk and safety report to the Risk and Safety Subcommittee. Clinical Patient Safety incidents 'causing harm' are reporting to the NRLS by the Clinical Governance team	Lisa J Tucker Health and Safety Manager

CONTENTS

Incident Reporting Procedure

1 Introduction

1.1 The Tavistock and Portman Foundation NHS Trust (the Trust) accepts that in the course of providing its services, adverse incidents can occur, some of which do, or could have serious consequences for patients, students, staff and the public. In such situations the immediate response will always be to care for the person affected and make the situation safe. Thereafter, the Trust has a responsibility to make every effort to reduce the likelihood of a re-occurrence by investigating incidents, understanding how they occur, and by taking appropriate preventive action.

1.2 The Trust recognises that most incidents occur because of problems with systems rather than with individuals. The Trust will ensure that timely and fair action is taken to manage incidents when they occur, to help prevent such incidents occurring in the future, by ensuring appropriate reporting, and by making subsequent improvements where indicated.

1.3 The Trust is committed to minimising unexpected adverse outcomes for patients, staff, students and visitors through the process of risk management. This incident reporting procedure aims to increase and maintain awareness of the need to identify and report incidents, near misses and serious untoward incidents.

1.4 Because of the nature of cyber incidents, an immediate response is often necessary in order to prevent escalation of the problem, please contact the IT Helpdesk and refer to the Cyber Security Incident Response Standard Operating Procedure and follow the directions therein as a priority over incident reporting.

2 Purpose

2.1 Requirement for Incident Reporting

This procedure is designed to ensure that the Trust has a consistent and effective method of incident reporting across its service, in accordance with national guidance and legislation. It sets out the steps that staff should follow to identify, record, and grade incidents, and sets out the system of escalation and investigation that is followed dependent on the risk score of the incident. This procedure should be read in conjunction with the Trust's Risk Management Policy and Strategy and the Serious Incident Procedure.

2.2 Fair Blame Statement

The Trust aims to take an integrated approach to learning from incidents of all types in order to improve its services. The Trust recognises that such learning can only take place in a non-threatening environment and that fear of disciplinary action may deter staff from reporting an incident. The Chief Executive has confirmed that no disciplinary action will result from reported incidents or mistakes, subject to certain exceptions:

- Incidents that warrant police prosecution of individual members of staff
- Incidents that reveal that actions of an individual are judged to be far removed from acceptable practice
- Repeated failure by a member of staff to report incidents
- Malicious uses of the reporting system

2.3 Raising Concerns

Staff should refer to the Raising Concerns and Whistleblowing Procedure if they feel the need to raise issue of patient safety, or other incidents, where they are concerned that the Trust is not acting. Staff are also reminded that they have a duty to report incidents and staff should have the expectation that the Trust will act appropriately in line with this procedure and the Serious Incident Management Procedure.

3 Scope

This procedure applies to all staff employed directly, or otherwise. This includes individuals with honorary contract arrangements, bank staff and agency workers.

This procedure applies to the reporting of accidents, incidents and near misses that affect the Trust's property or anyone affected in the course of its activities. When an accident or incident involves someone who is not a member of staff then it is the responsibility of the member of staff who is made aware of the accident or incident to follow the reporting requirements by completing an incident report. In addition staff should take steps to remove/ prevent access to residual hazards that may remain at the site of the accident/ incident so as to prevent further injury/ near miss incident.

This procedure applies to incidents of all types: clinical, non- clinical, health and safety and information governance incidents. All incidents must be reported centrally and the responsible manager will determine how the incidents will be managed and provide an action plan to prevent it re occurring.

National guidance on IG incidents differs from guidance on all other incidents and this is reflected in the processes and responsibilities.

4 Definitions

Term	Definition
Adverse Media attention	Media coverage or public concern about the organisation or the wider NHS.
Breach of confidentiality	Any incident involving the actual or potential loss of personal identifiable information that could lead to identity fraud, or have significant adversely affected individuals.

Term	Definition
Clinical Incident	An unplanned or unexpected event occurring during the course of investigation, treatment, or follow up, which gives rise to injury or harm to a patient, including safeguarding concerns, self-harm, attempted or suspected suicide.
Cyberspace	An interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services.
Dangerous occurrence	A serious failure of machinery, premises or plant as defined in RIDDOR. In addition to managing these incidents within the Trust the Health and Safety Manager must send a report to the Health and Safety Executive.
Data Loss	Loss shall mean the temporary or permanent inability to access or retrieve data.
Fire incident	Any event which results in, or had the potential, to damage people or property, or the accidental call for the Fire Brigade. These incidents are managed under the Trust's Fire Safety Policy.
Hazard	A hazard is a system and/or object that have the potential to cause harm.
Incident (or accident)	An unplanned or unexpected event that results in one or more of the following: causes an injury, either physical or psychological, to staff, patients/clients, visitors, volunteers, agency/bank staff or contractors results in damage to or loss of equipment, buildings, assets or structures that results in unplanned interruptions to service provision. A failure to comply with Trust policies.

Term	Definition
Information Governance Incident	Actual or potential failure to meet the requirements of the Data Protection Act and/or the common law of confidentiality, including misuse, unlawful disclosure, recording or sharing inaccurate data, information security breaches, and inappropriate invasion of privacy. Other IG incidents include breaches of the Freedom of Information Act or the Environmental Information Regulations.
Information Communication / Technology Incident	A system, service, device, or network failure which might lead to a failure of safeguards or compromise business continuity but has not resulted in an information incident.
Near miss	An incident in any of the categories listed above which does not result in injury or harm to persons or damage to property, but had the potential to do so. Near misses should be reported in the same way as incidents using the Trust's incident report
Personal confidential data	Any data from which an individual can be identified.
Reportable disease or injury	A work-related disease or condition listed in RIDDOR from which an employee or self-employed person is suffering and which has been confirmed by a medical practitioner or occupational health physician. This includes any injury or infection related to the workplace.
Security Incident	An unplanned or unexpected event which results in harm to persons or property, theft, break-in or wilful damage.
Serious Incident	These incidents are managed under the Trust's Serious Incident Procedure. An illustrative list of serious incidents is shown at Appendix A.

Term	Definition
Sharps Incident	Injuries caused by needle sticks, human bites, scratches or other injuries where the victim is at risk of contamination by human blood or body fluids. In the event of a sharps incident an incident report must be filled in and the victim should be managed under guidelines in the Trust's Infection Prevention and Control Procedure.
Staff	Any person undertaking the Trust's work, including employees, volunteers, students, and contractors.

5 Duties and responsibilities

The Chief Executive

The Chief Executive is responsible for the overall implementation, monitoring and revision of this procedure but in practice will delegate the operational management and oversight of this procedure to the Medical Director.

Medical Director

The Medical Director will be responsible for ensuring that a system is in place for investigating and follow up for all reported clinical incidents. They will also be responsible for ensuring external contact with the CSU's, CCGs, ICS or STP.

Also to ensure contact with the patients, and patient's families when the Trust decides to initiate, or be a part of an investigation of a serious incident and reporting any Serious Incident to the respective commissioner via the Strategic Executive Incident Solution (StEIS).

Associate Director of Quality and Governance

The associate director will be responsible for ensuring that a system is in place for investigating and follow up for all reported non clinical incidents. They will also be responsible for ensuring duty of candour requirements, liaison with commissioners and StEIS submissions are made for serious non clinical

incidents. To provide support to any other director for non-clinical serious investigations.

The associate director will work with the human resources service to ensure that adequate and appropriate training is provided to all staff on incident reporting and management.

Director of Information Management and Technology

The director will ensure that identified information threats and vulnerabilities are followed up for risk mitigation, and that perceived or actual cyber incidents are managed in accordance with NHS requirements.

Ensure that there are effective mechanisms in place for reporting and managing cyber Serious Incidents Requiring Investigation (cyber-SIRIs). These mechanisms should accommodate technical, operational or procedural improvements arising from lessons learned.

Assistant Director of IG & Data Security & Data Protection Officer

Holds the responsibility for logging any reportable IG incidents externally. They also have to check, review, investigate and close all IG incidents on the QP.

Directors

It is the responsibility of directors to disseminate this procedure within their area of responsibility and ensure its implementation by providing support and advice to their managers and staff. Promote incident reporting to their staff and ensure that recommendations arising from the analysis of incidents are actioned as appropriate within their directorate 'Sharing Lessons learnt'.

Line Managers

It is the responsibility of line managers to:

- Ensure that their staff understand and follow the incident reporting procedure
- Ensure that an incident report is completed for each incident/ accident correctly, and record any actions taken
- For a serious incident, to ensure that the incident is reported verbally to a senior management without delay, and the electronic incident form is completed, in accordance with the Serious Incident Procedure'

- Ensure that an identified incident is submitted electronically within 48 hours (part 1 and then part 2 of the form)
- Ensure that risk assessments are carried out (or reviewed) on all significant identified risks and put into place appropriate action plans to eliminate or reduce the risk to an acceptable level. The results of risk assessments must be communicated to all those who may be at risk and provided to their staff-side representative in writing if requested
- Liaise with the Health & Safety Manager regarding any safety or health issues related to the health and safety of any injured person
- Refer staff to the occupational health service where an incident results in an accident or injury. This will include events where a member of staff has been exposed to a hazardous substance.
- For all serious incidents, cooperate with senior managers and investigators to facilitate a full investigation and root cause analysis of the incident
- Implement any recommendations that are accepted following a serious incident.

The Assistant Director for Information Governance and Data Security

The Assistant Director is responsible for:

- Ensuring that information governance and security incidents are reported to the monthly Incident panel
- reported and considered at the Data Security and Protection Sub-committee of the Integrated Governance Committee, and that agreed actions are followed through
- Provide expert advice on IG and data security matters
- Assess and where necessary report serious IG incidents to the information Commissioner's Office (ICO), liaising with the Health and Safety Manager / Clinical Governance and Quality Manager for reporting on STEIS and to commissioners.
- Complete IG incident system administration processes, follow up on actions as required within 10 working days of submission.

The Health & Safety Manager

Is responsible for the administration of all non-clinical incidents, including health and safety across the Trust, and will provide advice and support to managers and staff on all aspects of incident management.

- Lead on all non-clinical incidents and monitor those that are reportable externally – to StEIS and Commissioners
- Ensure that all staff are aware of incident reporting requirements, using the Trust's electronic incident reporting system, the Quality Portal and that managers are completing and submitting part 2 of the incident form within 48 hours of the risk being identified
- Provide staff with help and advice on completing the electronic incident forms, and appropriate actions following an incident or near miss
- Ensure that serious incidents are reported to senior staff, actions taken to manage the incidents appropriately, where required appropriate authorities are informed and support the investigation as required, in line with the Serious Incident procedure
- Complete incident system administration processes which include checking each incident for correct category and scoring and follow up on actions as required within 10 working days of submission
- Produce reports for tracking progress of implementing action plans, and reports exploring trends where required, including to the Health and Safety working group
- Provide summaries of incidents (non-clinical and non IG) and reports from non-clinical Serious Incidents to the Incident panel
- Ensure all relevant patient safety incidents are uploaded to the National Reporting and Learning Data base (NRLS) weekly
- To deliver incident reporting and investigation training that meets current staff needs in liaison with HR.

Clinical Governance and Quality Manager shall:

- Lead on all clinical incidents and safeguarding incidents and monitor clinical incidents that are reportable externally – to StEIS , NRLS and Commissioners.

- Ensure that the clinical governance leads for the directorates are aware of the incident in their remit.

- Ensure timely delivery of the concise reports from Serious Incidents and action plans from Clinical incidents to the Incident panel.

- Complete clinical incident system administration processes which include checking each incident for correct category and scoring and follow up on actions

as required within 10 working days of submission

Provide quarterly Serious Incident Reports to the Trust Board.

Employees

It is the responsibility of employees to:

- Report all accidents / incidents on the Trust's incident reporting system the Quality Portal within 2 working days of the incident being identified, or for cyber security incidents, to IT helpdesk immediately
- The employee or the management should immediately inform the Trust's Health and Safety Manager and senior staff of any incident regarded as serious
- The person completing the incident report and the line manager should agree in the grading of the incident using the Trust's risk matrix

6 Procedures

6.1 Incident Reporting via the Trust's Quality Portal

All incidents are to be reported on the Trust's Quality Portal. This website can be accessed via the front page of the Trust intranet, or using the link on their PC desktop.

The witness to the incident, or an individual informed of the incident, is the person who completes part one, using factual details in the summary of incident section and ensuring there are no names and using initials.

The incident report must be completed and submitted as soon as possible after identifying the incident but not more than 2 working days. It should record the facts of the incident and not opinion. Further help on completing the report can be obtained from the Health and Safety Manager.

The person completing Part 1 of the incident form should grade the incident following the Trust's grading matrix. If the reporter is unclear about the grade then the matter should be referred to their manager or the Health and Safety Manager for further advice. The system provides guidance on grades.

In the event of any serious incident these should be immediately reported to the medical director, Director of technology and transformation and the service director

A manager to whom the report is directed completes Part 2 of the incident report, and should have some response and action plan in place.
The report can have extra information added to it at any time, including updates and attaching reports. All email correspondence should be sent via the portal as this is then logged against the incident.

All Standard Operating Procedures for all aspects of incident reporting on the Quality Portal can be found in the training module on the QP

Please be aware that the QP can time out whilst you complete a report, it is advised if there is if the QP isn't working or you have concerns about the amount of information you are adding to the report so save it as a separate word document, or as a follow up email, and then cut and paste the information onto the QP.

6.2 Action to be taken by the Health and Safety Manger

On receipt of the incident report, the Health and Safety Manager will review it for completeness, obtain further information if required and review the grade recorded on the incident report. If grading is incomplete or questionable the Health and Safety Manager will review the grading with the reporter and the relevant manager.

6.3 Duty of Candour

'Every healthcare professional must be open and honest with patients when something that goes wrong with their treatment or care causes, or has the potential to cause, harm or distress. If the level of harm to the patient is moderate to severe, then the duty of candour must be applied. The duty of candour involves sending a letter to the affected patient (or, where appropriate, the patient's advocate, carer or family) offering sympathy, acknowledging the harm or potential harm the incident may have had on the patient during their care at the Trust, and assuring them that the incident will be investigating and providing all appropriate investigation details.

Incidents requiring duty of candour can range from a patient death by suicide to an unauthorised data disclosure with negative associated consequences, again leading to moderate or severe harm or potential harm to the patient.

6.4 Investigation

The degree of investigation of an incident will be determined by reviewing the incident severity and potential for learning lessons, national serious incident guidance or by the IG SIRI criteria (for all IG incidents). The Medical Director will take the decision for clinical incidents and the IMT Consultant for non-clinical incidents.

6.5 Additional reporting

Mandatory requirements direct that certain categories of incidents are reported to various external agencies e.g. the Health and Safety Executive (RIDDOR reporting), the National Reporting and Learning System (NRLS) and the Medicines and Healthcare Products Regulatory Agency (MHRA).The Health and Safety Manager is responsible for making these reports according to their role.

6.6 Reporting procedure for non-Trust employees who have an incident or accident on Trust property

Patient/service-users

All accidents/incidents involving patients are to be reported by a member of staff on the Quality Portal in accordance with the process detailed above.

Contractors

Contractors are responsible for reporting any accidents/incidents directly to their employer or the enforcing authority if necessary using their own company reporting systems.

To enable the Trust to monitor activities taking place on its properties copies of any such incidents involving contractors or self-employed persons must also be forwarded to the Health and Safety Manager to be used for information purposes.

Students

If a student is on placement with the Trust and has an accident the staff member responsible for that student during the placement must report the matter to the university/college from where the student came as soon as possible in addition to completing the Trust's incident report.

Visitors to Trust sites

If a visitor is injured or harmed whilst on site the appropriate first aid should be provided and any practical assurance required. An Incident Report should be completed by the member of staff witnessing the accident or by the first aider.

6.7 Legal, Statutory and Stakeholder Reporting

These arrangements are summarised in the table below:

Risk level	Escalation level	Initial reporting	Level of Investigation	Review
Extreme Red 15- 25	Board	Complete incident report Inform CE and leads in appendix G Following SI Procedure Health & Safety Manager to ensure all appropriate agencies (HSE, NPSA etc.) are informed Associate Director of Quality and Governance to report via STEIS.	Conduct full investigation and root cause analysis following the Serious incident Procedure Consideration and decision of who is to contact the patient or patient's family and inform them of the investigation.	CEO and/or Medical Director to ensure all relevant external agencies are informed in accordance with the Serious Incident Procedure. Clinical Governance Manager to ensure Clinical Incident review is carried out Findings/ recommendations to go EMT
High Orange 9-12	Executive Management Team (reporting to Board)	Complete incident report Following SI Procedure Health & Safety Manager to ensure all appropriate agencies (HSE, NPSA etc.) are informed and record on database	Conduct a preliminary investigation and consider a full investigation and root cause analysis following the Serious incident Procedure Consideration and decision of who is to contact the patient or patient's family and inform them of the investigation.	Clinical Governance Manager to ensure Clinical Incident review is carried out Findings and / or recommendations to go appropriate committee

Risk level	Escalation level	Initial reporting	Level of Investigation	Review
Moderate Yellow 6-8	Directorate/ Department	Complete incident report inform line manager Inform Health & Safety Manager, Health & Safety Manager t to ensure all appropriate agencies (HSE, NPSA etc.) are informed and record on database	Line Manager and Health and Safety Manager to decide any further preventative actions or the need for a local investigation.	Review risk assessments if required, i.e. if any action taken following investigation
Low Green 1-5 (tolerated risks)	Department, but monitored at Directorate level	Complete incident report with a line manager completing section two on any actions taken or to be taken, H&S Manager to ensure all appropriate agencies (HSE, NPSA etc.) are informed and record on database	No further investigation normally instigated unless felt required by Line Manager Re-grade if required following any investigation	Review risk assessments if required

6.8 IG and Data Security Incidents

IG and data security incidents will be assessed for seriousness by the Assistant Director for Information Governance and Data Security. If the result is that the score is less than 2, then this procedure applies otherwise, the HSCIC guidelines apply. All serious incidents to be reported to the Information Commissioners Office.

7 Training Requirements

7.1 Training

The Trust recognises that training of all staff is an essential to the effective working of this incident reporting procedure.

The responsibility for training in incident reporting lies with the Health and Safety Manager.

The Trust has determined that training needs to be provided at a basic level for all staff and at a higher level for key staff in the trust. The format of training that will be made available is as follows:

- All new staff will receive an introduction to the Trust's approach to incident reporting as part of basic induction
- All staff will receive update training on incident reporting which may be through classroom based or e-learning.
- Managers and Senior Staff will receive specific training on incident reporting and investigation as part of on-going in-service training for managers

Training will be provided by internal staff with appropriate skills, alternatively the Trust can use external skilled trainers to provide serious incident investigation training.

The training providers will monitor and report attendance as appropriate and ensure that attendees evaluate each session to ensure learning objectives are met and improvements to future sessions can be made.

8 Process for monitoring compliance with this Procedure

8.1 Regular Reporting

In order to assess compliance with this procedure and to ensure that the Trust learns from incidents that occur in the course of its business the following routine reviews will be undertaken:

- Monthly reports to the Incident panel from the Health and Safety Manager, Clinical Governance Team and Assistant Director for Information Governance and Data Security
- Quarterly report on all incidents to the Integrated Governance Committee, or a sub- committee that scrutinises assurance on its behalf. This may result in segmentation of clinical, non-clinical and information governance and data security incidents.

The work streams will monitor the effectiveness of incident management and may make recommendations for changes to practice or procedures based on reports received.

8.2 Risk Register

Where incidents indicate an on-going risk to the trust following investigation and treatment a Risk Assessment should be undertaken to determine if the risk should be entered onto the Trust's risk register together with details of the on-going action/treatment plan. See the Risk Management Procedure for details. The risk register will be reviewed by the Board of Directors, Management Team and Directors, as appropriate to level of risk indicated.

8.3 Serious Incident Monitoring

Compliance with incident reporting and investigation requirements for serious incidents will be monitored under the serious incident procedure.

9 References

Department of Health. (2000). *An Organisation with a Memory: Report of an Expert Group on Learning from Adverse Events in the NHS*. London: Department of Health.

Department of Health. (2001). *Building a Safer NHS for Patients: Implementing an Organisation with a Memory*. London: Department of Health.

Health & Safety Executive. (1995). *Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR Explained, Version 6)*, Suffolk: Health and Safety Executive. Available at: www.hse.gov.uk

Duty of Candour - Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 20.

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

National Patient Safety Agency. (2005). *Building a Memory: Preventing Harm, Reducing Risks and Protecting Patient Safety* London: National Patient Safety Agency.

Health and Safety (Consultation with Employees) Regulations 1996. (Statutory Instrument 1996 No. 1513). London: The Stationery Office. Available at: www.opsi.gov.uk

Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation
https://nww.igt.hscic.gov.uk/resources/IGIncidentsChecklistGuidance.pdf

10 Associated Documents

The procedure should be read in conjunction with the following policies as appropriate:

- Risk Management Policy and Strategy
- Risk Management Procedure
- Serious Incident Procedure
- Major Incident Plan
- Raising Concerns and Whistleblowing Procedure
- Health and Safety Policy
- Infection Prevention and Control Procedure
- Fire Safety Policy
- Business Continuity Plan.

- Information Governance Framework [see IG Policy]

Appendix A: Serious Incidents

Serious Incidents

The following is an *illustrative list* of examples of serious incidents. These are managed under the **Trust's Serious Incident Procedure.**

- An accident or incident involving a patient, member of staff, visitor on Trust property, contractor or other person, to whom the Trust owes a duty of care, occurs causing serious injury or death.
- A patient causes serious harm to another person whilst on premises and/or under care to the Trust
- Serious damage occurs to Trust property as a result of fire, flood, criminal activity etc.
- Large-scale theft or fraud has occurred or major litigation is likely or expected.
- A serious work-related disease or condition listed in RIDDOR from which an employee is suffering and which has been confirmed by a medical practitioner or Occupational Health Physician.
- Serious breach of confidentiality or data loss , all IG incidents
- Adverse Media Attention
- Allegation of Abuse , Assault or Safeguarding

Appendix B: Risk Matrix

The following definitions can be found on the electronic incident form when you hover over the relevant 'consequence' boxes

Descriptor/ Grade	CONSEQUENCE/IMPACT DESCRIPTION
Negligible (1)	**Negligible impact** on strategic objectives **Nil/negligible:** Injury loss service interruption environmental/estate impact impact on reputation impact on quality litigation or complaint non-identifiable data loss.
Low (2)	**Small variance** from overall strategic objective. First aid treatment with full recovery. Complaint possible Local low key external interest. **Minor:** financial loss (up to 5k) service interruption adverse effect on environmental/estate adverse effect on reputation adverse effect on quality. Loss of individual machine, system, network, applications up to half a day minor breach of confidentiality, where no sensitive data was disclosed/lost.
Moderate (3)	**Notable negative variance** from overall strategic objective. Medical treatment required up to 3 months to recover Reportable under RIDDOR complaint probable. **Moderate :** financial loss (5K – 200k) service interruption for more than one week adverse effect on environmental/estate adverse effect on reputation. Local press, stakeholders express concern adverse effect on quality temporary loss or mis-location of data internally moderate risk of low value claim. Loss of individual machine, system, network, applications over half a day loss of several machines, systems, networks, applications up to half a day breach of confidentiality involving sensitive data
Major (4)	**Significant variance** from overall strategic objective. Long term illness or injury (up to one year) Reportable under RIDDOR Complaint expected/received. **Major :** financial loss (200k – 3m) service interruption of more than one month adverse environmental/estate conditions leading to loss of service significant adverse effect on reputation significant medical intervention required for more than one week, significant concerns raised by stakeholders significant adverse effect on quality, including risk of failing to meet CQC standards. High value claim action by HSE anticipated moderate risk of high value claim. Loss of one or more non-patient activity networks, systems, applications for more than one day loss of one or more patient activity networks, systems, applications for more than half a day permanent loss of non-patient data significant breach of confidentiality involving sensitive data which caused the subject distress.

Extreme/ Catastrophic (5)	**Failure to meet strategic objective threatens independent functioning** or stability of the Trust. Death and/or Financial loss3M+ **Certain** : risk to reputation, national press 3+ days, risk of questions in the House of Commons. **Serious/long term and/or permanent** loss of information that impacts directly on service delivery Quality- External controls exerted; threat of Judicial Review, expected litigation valued at 1M+ High profile breach of confidential information (e.g patient identity). Buildings/property condemned leading to major loss of service. Permanent patient data loss severe breach of confidentiality involving sensitive data, caused distress, and involved over 10 individuals.

The likelihood score is determined by a judgement of the chance of the event occurring or recurring.

Score	Descriptor	Likelihood of repeat event
1	**Very unlikely to occur**	Will only occur in exceptional circumstances.
2	**Unlikely to occur**	Unlikely to occur but the potential exists.
3	**Could occur**	Reasonable chance of occurring has happened before on occasion.
4	**Likely to occur**	Likely to occur – strong possibility.
5	**Almost certain to occur**	The event is expected to occur in most circumstances.

Risk Score Matrix

Likelihood	Almost certain to occur	5	5	10	15	20	25
	Likely to occur	4	4	8	12	16	20
	Could occur	3	3	6	9	12	15
	Unlikely to occur	2	2	4	6	8	10
	Very unlikely to occur	1	1	2	3	4	5
Risk Matrix			1	2	3	4	5
			Negligible	Minor	Moderate	Major	Catastrophic /Fatal
			Consequence				

RISK SCORE = Consequence score x likelihood score

Appendix C: RIDDOR Reportable Incidents

Reportable injuries or events to the Health & Safety Executive (HSE) under RIDDOR.

Under RIDDOR, it is an offence to fail to report an event reportable under the RIDDOR criteria, or by failing to report with the specified periods. The Health and Safety Manager will report any incident that falls under these regulations.

What has to be reported?
Incidents falling within the below criteria involving staff, patients, contractors and visitors.

The event types that are required to be reported under RIDDOR are:

- deaths
- major injuries
- accidents at work resulting in over 5 days off of work
- dangerous occurrences
- gas incidents

Keeping Records

The Trust must keep a record of any reportable injury, disease or dangerous occurrence. This must include the date and method of reporting the date, time and place of the event, personal details of those involved and a brief description of the nature of the event or disease. You can keep the record in any form you wish.

Appendix D : Equality Impact Assessment

Completed by	**Lisa Tucker**
Position	**Health and Safety Manager**
Date	**13.06.2020**

The following questions determine whether analysis is needed	**Yes**	**No**
Does the policy affect service users, employees or the wider community? The relevance of a policy to equality depends not just on the number of those affected but on the significance of the effect on them.		X
Is it likely to affect people with particular protected characteristics differently?		X
Is it a major policy, significantly affecting how Trust services are delivered?		X
Will the policy have a significant effect on how partner organisations operate in terms of equality?		X
Does the policy relate to functions that have been identified through engagement as being important to people with particular protected characteristics?		X
Does the policy relate to an area with known inequalities?		X
Does the policy relate to any equality objectives that have been set by the Trust?		X
Other?		X

If the answer to *all* of these questions was no, then the assessment is complete.