

P2

INCIDENT MANAGEMENT POLICY AND PROCEDURE

INCIDENT MANAGEMENT POLICY AND PROCEDURE

Kingston CCG Policy Reference: IMP/1/16

This policy replaces or supersedes Policy Ref: CA004

THIS POLICY HAS BEEN APPROVED BY KINGSTON CCG AND WILL HAVE EFFECT AS OF August 2016

Target Audience	Governing Body members, committee members and all staff working for, or on behalf of, the CCG
Brief Description (max 50 words)	This policy sets out the principles by which the CCG will manage the reporting of all types of incidents, including near misses. Reporting of near misses where there has been no actual injury or loss may enable appropriate action to be taken to prevent future incidents.
Action Required	<p>Following approval at the CCG Governing Body, The Chief Officer will ensure that the requirements of this policy will be raised at all team meetings, and confirm the requirements with the chairs of each committee, and with CCG executives.</p> <p>Chairs of committees will identify the programme of review with the Accountable Executive for each policy within their committee remit.</p> <p>Accountable Executives will identify policy owners for each policy within their remit.</p> <p>The Governance Lead will establish and maintain a corporate register of all policies and their status, and will ensure that these are appropriately reflected on the website.</p>

Approved: Integrated Governance Committee on 26th July 2016
Review date: July 2019

Document Control	
Title:	Incident Management Policy and Procedure
Original Author(s):	Jill Pearse, Information Governance Lead
Owner:	Director of Quality and Governance
Reviewed by:	Fergus Keegan, Director of Quality & Governance
Quality Assured by:	Integrated Governance Committee
File Location:	GPTeamNet
Approval Body:	Integrated Governance Committee
Approval Date:	August 2016

Document Review Control Information

Version	Date	Reviewer Name(s)	Comments

Document Information

Title /Version Number/(Date)	Incident Management Policy and Procedure / Version 1 /July 2016
Document Status (for information/ action etc.) and timescale	For implementation July 2016
Accountable Executive	Director of Quality and Governance
Responsible Post holder/Policy Owner	Head of Information Governance
Date Approved	5 August 2016
Approved By	Integrated Governance Committee
Publication Date	8 August 2016
Review Date	August 2019
Author	Head of Information Governance
Stakeholders engaged in development or review	Director of Quality and Governance Integrated Governance Facilitator Customer Services Officer Executive Business Lead Staff Side Representative Chair of Integrated Governance Committee Quality Manager
Equality Analysis	<p>Equality Analysis</p> <p>This Policy is applicable to the Governing Body, every member of staff within the CCG and those who work on behalf of the CCG. This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010. This document demonstrates Kingston CCG's commitment to create a positive culture of respect for all individuals, including staff, patients, their families and carers as well as community partners.</p> <p>The intention is, as required by the Equality Act 2010, to identify, remove or minimise discriminatory practice in the nine named protected characteristics of age, disability, sex, gender reassignment, pregnancy and maternity, race, sexual orientation, religion or belief, and marriage and civil partnership. It is also intended to use the Human Rights Act 1998 and to promote positive practice and value the diversity of all individuals and communities.</p>
Contact details for further information	

Associated Policy Documents

Reference	Title
	Serious Incidents Policy
	Health and Safety Policy
	Anti-Fraud and Anti-Bribery Policy
	Whistleblowing policy
	Information Governance Policy

Glossary

Term	Definition
Accountable Executive	CCG Executive accountable for development, implementation and review of the policy
Policy Owner	Post holder responsible for the development, implementation and review of the policy
Document definitions	These are provided in Section 7

1. INTRODUCTION

- 1.1 For any risk management strategy to work, potential and actual risks and incidents must be reported and action taken to prevent a recurrence. This policy covers the reporting of all types of incidents, including near misses. Reporting of near misses where there has been no actual injury or loss may enable appropriate action to be taken to prevent future incidents. For ease of reference this policy is a separate document to the Kingston CCG Serious Incident Policy and Procedure; however the two policies should be read in conjunction.
- 1.2 The CCG has a responsibility for managing risks identified in the commissioning process to ensure the quality of the services it commissions is safe and of a high standard. The CCG also has a responsibility to ensure their contractors have effective systems in place to identify and manage risks and incidents and support them in the development of these where necessary. Further, they need to act as a conduit for information about such risks and incidents, to ensure that the learning (and the opportunities for risk reduction) from them is not lost within the CCGs or the wider NHS.
- 1.3 This policy covers the broad categories as follows:
- corporate business incidents
 - health and safety / fire / security or environmental incidents
 - Information Governance Incidents
 - IT (Information Technology) Incidents
 - Clinical quality incidents

2. RATIONALE

‘Building a Safer NHS for Patients’ identifies four types of incidents that need to be reported: errors; near misses, adverse events and serious incidents (SI’s). This document takes into account guidance from the Department of Health, National Patient Safety Agency and the NHS Litigation Authority.

3. POLICY SCOPE

- 3.1 This policy shall apply to all staff working for and on behalf of Kingston CCG (including locum, contractors and agency staff), students on placements, volunteers and directly commissioned staff e.g. the South East Commissioning Support Unit. It must be used for all incidents and near misses that affect patients, clients, staff, external contractors or visitors, either on Kingston CCG premises or witnessed/noticed by employees in the course of their duties but outside Kingston CCG premises and services. In addition, this policy and procedure provides a framework that can be adapted and/or adopted by our independent contractors.

4. EQUALITY IMPACT ASSESSMENT

In applying this policy, the CCG will have due regard for the need to eliminate unlawful discrimination, promote equality of opportunity, and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or any other personal characteristic.

An equality impact screening assessment has been completed (Appendix 8) and no negative impacts were identified. The positive impacts support the CCG's equality objectives

5. OBJECTIVE

To ensure the CCG reports incidents in line with national requirements, takes appropriate action to learn from these and implements any actions to reduce the impact and mitigate the risk of re-occurrence.

6. JUST SAFETY CULTURE STATEMENT

- 6.1 Kingston CCG operates under a 'Just Safety Culture'. To foster a just safety climate culture, no disciplinary action will result from the reporting of an incident, mistake, SI or near miss, except where there has been criminal or malicious activity, professional malpractice, acts of gross misconduct, repeated mistakes or where errors or violations have not been reported.
- 6.2 As an organisation, we are aware that accidents, incidents, SIs and near misses can and do happen from time to time. Lessons need to be learned from these events in order that every effort is made to prevent a recurrence.
- 6.3 When an incident is reported it can be a stressful time for anyone involved, whether they are members of staff, a patient directly involved or a witness to the incident. They all need to know that they are going to be treated fairly and that lessons will be learned and action taken to prevent the incident happening again.
- 6.4 During an incident investigation, appropriate support will be offered to staff and anyone else involved in the incident if required. Support includes access to counselling services and the provision of regular updates of the investigation and its outcomes. Information is available on request from the Governance Team.

7. DEFINITIONS & ACRONYMS

7.1 Incident

An incident is a single distinct event or circumstance that occurs within the organisation which leads to an outcome that was unintended, unplanned or unexpected.

The incident could also occur outside the organisation if a member of staff is visiting other locations in the course of their work.

Incidents are often negative by nature but can also include positive leaning events which can be shared throughout the organisation as good practice.

An incident could involve:

- environment (workplace)
- organisational reputation
- property
- service delivery staff
- stakeholder

7.2 Serious Incident

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

The occurrence of a serious incident demonstrates weaknesses in a system or process that need to be addressed to prevent future incidents leading to avoidable death or serious harm to patients or staff, future incidents of abuse to patients or staff, or future significant reputational damage to the organisations involved.

Serious incidents therefore require investigation in order to identify the factors that contributed towards the incident occurring and the fundamental issues (or root causes) that underpinned these. Serious incidents can be isolated, single events or multiple linked or unlinked events signalling systemic failures within a commissioning or health system.

Please refer to Serious Incident Policy for further details

7.1 Serious Incident Requiring Investigation (SIRI)

Incidents falling into this category are essentially information governance or IT security related. (See appendix 2)

7.3 Never Event

All Never Events are defined as serious incidents although not all Never Events necessarily result in serious harm or death. See [Never Events Policy and Framework](#) for the national definition and further information;

7.4 Near Miss

An incident could be a **near miss** which is an event or situation that has the potential to cause harm but which never happened. These events should also be reported so the organisation can learn lessons and take preventative action where required.

7.5 Harm

Harm is defined as an injury (physical or psychological), disease, suffering disability or death. In most circumstances harm can be considered to be unexpected, rather than the natural cause of the patient's underlying condition

7.6 RCA (Root Cause Analysis)

RCA is a systematic process whereby the factors that contributed to an incident are identified. As an investigation technique for incidents, it looks beyond the individuals concerned and seeks to understand the underlying causes and environmental context in which an incident happened.

7.7 National Reporting and Learning System (NRLS)

The NRLS is a central database of **patient safety incident reports**.

7.8 The Medicines and Healthcare products Regulatory Agency (MHRA)

The MHRA regulates medicines, medical devices and blood components for transfusion in the UK. It is an executive agency, sponsored by the Department of Health.

7.9 Datix

Local incident reporting system and adverse event reporting used by Kingston CCG

7.2 Strategic Executive Information System (STEIS)

The National **serious incident** on-line reporting system.

7.3 RIDDOR

The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013. RIDDOR puts duties on employers, the self-employed and people in control of work premises (the Responsible Person) to report certain serious workplace accidents, occupational diseases and specified dangerous occurrences (near misses). (See appendix 4)

7.4 HSCIC

The Health and Social Care Information Centre. Maintains the central database of information SRI incident reports

8. TYPES OF INCIDENTS

The following are examples of types of incidents used in this document:

- Personal accident
- Clinical incident
- Business Continuity Incident
- Corporate Business Incidents
- Information governance/Breach of confidentiality
- Fire incident
- Security Estates and Environmental Incidents
- Health and Safety
- Staff Ill Health
- Violence/abuse/harassment
- Vehicle incident
- Health & safety
- Other (Not included in above)

Note that incidents may fall under more than one category.

8.1 Personal accident

Accidents/incidents where a person is injured – examples include slips, trips and falls, and injuries to persons

8.2 Clinical Incidents

A clinical incident is any unintended or unexpected incident which could have led to or did lead to harm for one or more patient's receiving NHS care.

8.3 A Business Continuity Incident

An unwanted event that threatens personnel, buildings, operational procedures or the reputation of the organisation which requires special measures to be taken to restore things back to normal.

8.4 Corporate Business Incidents

A corporate business incident is an event or circumstance that could have or did have a negative impact on the way the CCG does business with their, stakeholders and that could lead to financial loss.

8.5 Fire

Fire outbreak, false alarm

8.6 Security, Estates and Environmental Incidents

- **security** - could involve damage, loss, theft
- **estates/facilities** - could include a water leak, a lack of electricity occurring in buildings
- **environmental** – impact on land, air or watercourses

8.7 Health and Safety

This will include RIDDOR reportable incidents (see appendix 4)

8.8 Staff ill health

Incidents of this type could include seizures, work related disorders

8.9 Violence/abuse/harassment

Any act in which a person is abused, threatened, intimidated or assaulted in his or her employment. Workplace violence includes:

- Threatening behaviour - such as shaking fists, destroying property or throwing objects.
- Verbal or written threats - any expression of an intent to inflict harm.
- Harassment - any behaviour that demeans, embarrasses, humiliates, annoys, alarms or verbally abuses a person and that is known or would be expected to be unwelcome. This includes words, gestures, intimidation, bullying, or other inappropriate activities.
- Verbal abuse - swearing, insults or condescending language.
- Physical attacks - hitting, shoving, pushing or kicking.

Rumours, swearing, verbal abuse, pranks, arguments, property damage, vandalism, sabotage, pushing, theft, physical assaults, psychological trauma, anger-related incidents, rape, arson and murder are all examples of workplace violence.

Workplace violence is not limited to incidents that occur within a traditional workplace. Work-related violence can occur at off-site business-related functions (conferences, trade shows), at social events related to work, in clients' homes or away from work but resulting from work (a threatening telephone call to your home from a client).

8.10 Vehicle incident

Incidents involving vehicles whilst on CCG business

8.11 Information Governance Incidents

An information governance incident is an event or circumstance which affects or could affect the security of the information maintained by the CCG.

IG incidents will fall into one of the following cause groups:

- breach of confidentiality
- damage to hard copy records
- inappropriate access to/or disclosure of a person's information
- information left unattended (printer, empty office)
- lost/stolen – equipment
- misdirected email containing confidential information
- email containing confidential information sent through insecure route
- misdirected hardcopy (e.g. post, fax etc.)
- password sharing

All Organisations processing Health, Public Health and Adult Social Care personal data are required to use the IG Toolkit Incident Reporting Tool to report level 2 IG SIRIs to the DH, ICO and other regulators. This has been a requirement since 1st June 2013.

8.12 Information Technology (IT) Incidents

An information technology (IT) incident is an event or circumstance that affects or could affect the way the CCG does business negatively and is attributed to IT systems and/or the network.

These incidents will most often include, but are not limited to:

- hardware failure
- network failure
- software failure
- server failure
- telecommunications failure
- virus discovery

9. MANAGEMENT OF INCIDENTS

9.1 Discovering an incident

On discovery of an incident the primary concern is to ensure the immediate safety of patients, staff and the public. If the incident is serious, or if an emergency situation arises, the Director of Quality and Governance must be contacted immediately and the Serious Incident Policy must be followed.

9.2 Classifying the risk

The person involved in or witness to the incident must immediately make an initial assessment of the actual impact that the incident has had. This will be one of five levels: insignificant, minor, moderate, severe or catastrophic. The initial impact of the incident will inform the immediate reporting requirements (see appendices 1 and 2).

In all cases the line manager signing off the incident report form must confirm the actual impact and also make an assessment of the likelihood of recurrence of the incident using the matrix and guidance below. The process for using the classification system is described clearly in the incident report form and will inform the level of investigation that must occur. (See appendix 1)

Information Governance and Cyber Security incidents have a separate classification procedure and must be treated in accordance with [guidance](#) provided by the Health and Social Care Information Centre (HSCIC) (see appendix 2)

Advice on grading an incident can be sought from the Director of Quality & Governance if needed. The classification of the incident may change at any time and may become higher or lower. The management of the incident may change if the grading changes.

9.3 Local Incident reporting

- 9.3.1 All Incidents and near misses must be reported in accordance with the following procedure. Incidents classified as serious incidents must follow the Serious Incidents Policy.
- 9.3.2 Depending on the level of actual impact, the member of staff must inform the following people within the timescales laid out below:

Actual impact	Who to inform	Timescale
Insignificant	Line Manager (or nominated person in charge)	Within one working day
Minor	Line Manager (or nominated person in charge)	Within one working day
Moderate	Line Manager (or nominated person in charge)	Immediately
Severe	Person in Charge who will then decide whether serious enough to contact the On-call Director)	Immediately
Catastrophic	Director of Quality & Governance or On-call Director	Immediately

- 9.3.3 An incident report form (see appendix 6) must be completed and signed within one working day of the incident and countersigned by the line manager (or nominated person in charge) who must also confirm the impact and make an assessment of the likelihood of recurrence.
- 9.3.4 Incident reports must only contain known facts. Opinions should not be recorded.
- 9.3.5 Where a patient has been affected by the incident, details should also be recorded within the patient record.

- 9.3.6 On completion, all incidents forms, once signed by the line manager, must be sent to the Customer Care officer within three working days of the incident occurring, and to the Quality Manager within one working day if a serious incident.

9.4 External Reporting requirements

- 9.4.1 Incidents classified as **Serious Incidents** (see Serious Incidents Policy) must be reported to NHS England via STEIS via the Quality Manager
- 9.4.2 **SIRIs** must be reported to the DH (Department of Health) and the ICO (Information Commissioners Office) on the Health and Social Care Information Centre Information Governance Toolkit via the Senior Information Risk Owner (SIRO) (Director of Quality and Governance)
- 9.4.3 **RIDDOR** reportable Incidents (See appendix 4) must be reported to the Health and Safety Executive on the [RIDDOR](#) reporting system via the Director of Quality and Governance
- 9.4.4 **Medicines**
The system for reporting medication error incidents in England is the NRLS.

The Medicines and Healthcare products Regulatory Agency regulates medicines, medical devices and blood components for transfusion in the UK.

MHRA is an executive agency, sponsored by the Department of Health. MHRA and NHS England are working together to improve the quality and extent of reporting, and the resulting learning, in the field of medication errors. As part of this partnership, the NRLS will be an integrated reporting route for medication error incidents, see figure two below.

Suspected ADRs not involving medication errors reported via the NRLS should continue to be sent directly to the MHRA through the Yellow Card Scheme. It is good practice to share copies of submitted Yellow Card reports with the MSO for local learning and action.

Near-miss incidents that have not caused harm but have the potential to do so and those involving errors of omission will stay in the NRLS and be used by the Patient Safety Domain in NHS England for national learning.

9.5 Investigation of Incidents

Where incidents are sufficiently serious or complex, or part of an ongoing pattern, a formal investigation may need to take place to establish the root cause of the incident.

The level of investigation, guided by the level of risk presented by the reported incident, should be determined as part of the reporting procedure by both the reporter and the Incident Investigating Manager. However, it should be noted that as individual incidents can vary, so too can the level of investigation required.

The standard approach to the investigation of any incident occurring within the organisation is to apply the principles of a Root Cause Analysis (RCA) to establish the true reasons for the incident so they may be prevented in the future. Refer to the RCA guidance (see appendix 3).

9.5.1 **Levels of Investigation**

It is the responsibility of the CCG to ensure that an appropriate investigation takes place following an incident or near miss according to the severity and possible implications of the incident. It is important to note that:

- All losses and compensations must be investigated
- All potential claims and complaints must be investigated

If the incident occurred within a different organisation, the incident must still be reported for appropriate investigation and a decision made as to the most appropriate lead for the investigation.

Incidents with an impact assessment of 1 to 3 may not require further action other than that specified in the initial incident form (see appendix 1). Reassessment of any residual risk must be carried out after the implementation of any actions. For incidents with an impact assessment of 4 or 5, an investigation must always be carried out. - all incidents meeting the threshold of a serious incident must be investigated and reviewed according to principles set out in the Serious Incidents Policy.

The standard approach to the investigation of any incident occurring within the organisation is to apply the principles of a Root Cause Analysis (RCA) to establish the true reasons for the incident so they may be prevented in the future. Refer to the RCA guidance (see appendix 3).

10. **TREND ANALYSIS / LEARNING LESSONS**

An overview of incidents reported across the organisation will be monitored for trends, themes and lessons learned through a number of committees, groups and meetings. The Integrated Governance Committee has responsibility of maintaining oversight incident management and will receive quarterly reports of all reported incidents. Depending on the type of incident other committees will also receive specific reports as shown in the table below

Type of Incident	Committee
Information Governance/Breach of Confidentiality	Information Governance Steering Group
Information Technology/Cyber crime	Informatics and Information Technology Steering Group
Fraud and Bribery	Audit Committee
Health & Safety	Joint Health & Safety Committee

11. DUTIES AND RESPONSIBILITIES

Chief Officer	The Chief Officer has overall responsibility for the strategic direction and operational management, including ensuring that CCG process documents comply with all legal, statutory and good practice guidance requirements.
Director of Quality & Governance	<p>The Director of Quality & Governance has overall responsibility for ensuring:</p> <ul style="list-style-type: none">the incident management process is robust and adhered toincidents are maintained and managed in timely mannerstaff have the necessary training required to implement the policymechanisms are in place within the organisation for regular reporting and monitoring of incident themes and lesson learned
Managers	<p>Managers have the responsibility:</p> <ul style="list-style-type: none">to support their directors and staff to maintain the incident policy and to manage individual incidents in accordance with policyto work closely with the Director of Quality & Governance to ensure a transparent and consistent approach to incident management across the CCG in partnership with key stakeholders <p>All managers and supervisory staff are responsible for the adherence and monitoring compliance within this policy.</p>
All Staff	<p>All staff, including temporary and agency staff, are responsible for:</p> <ul style="list-style-type: none">Compliance with relevant process documents. Failure to comply may result in disciplinary action being takenCo-operating with the development and implementation of policies and procedures as part of their normal duties and responsibilitiesIdentifying the need for a change in policy or procedure as a result of becoming aware of changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising there line managerAttending training/awareness sessions when provided

12. IMPLEMENTATION

This policy will be available on the GPTeamNet for all staff, for use in the reporting and management of incidents and near misses.

CCG directors and managers are responsible for ensuring that relevant staff within the CCG have read and understood this document and are competent to carry out their duties in accordance with the procedures described.

13 TRAINING IMPLICATIONS

The training required to comply with this policy is key to the successful implementation of the policy and embedding a culture of incident reporting and management in the organisation. Through a training and education programme, staff will have the opportunity to develop more detailed knowledge and appreciation of the role of incident reporting and management.

The Director of Quality & Governance will ensure that the necessary training or education needs and methods required to implement the policy are identified and resourced or built into the delivery planning process. This may include identification of external training providers or development of an internal training process.

The level of training required in incident reporting and management varies depending on the level and responsibility of the individual employee.

Training and education will be offered through a rolling programme of incident reporting and management training.

14 LEGISLATION, STATUTORY REQUIREMENTS AND NATIONAL GUIDANCE

[Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation](#) – May 2015

[Information Governance Incident Reporting Tool User Guide](#)

[NHS England Serious Incident Framework March 2015](#)

[No secrets: Guidance on developing and implementing multi-agency policies and procedures to protect vulnerable adults from abuse](#) (Department of Health) 2000

[RIDDOR - Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013](#)
<http://www.hse.gov.uk/riddor/>

15 MONITORING AND REVIEW

15.1 Monitoring

The Director of Quality and Governance will oversee, on behalf of the Integrated Governance Committee, the monitoring the dissemination and implementation of this policy.

A detailed quarterly report will be reviewed by the Integrated Governance Committee

15.2 Review

The CCG Integrated Governance Facilitator will ensure that each policy document is reviewed in accordance with the timescale specified at the time of approval. No policy or procedure will remain operational for a period exceeding three years without a review taking place.

Staff who become aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives that affect, or could potentially affect policy documents, should advise the Director of Quality and Governance as soon as possible, via line management arrangements. The Director of Quality and Governance will then consider the need to review the policy or procedure outside of the agreed timescale for revision.

Appendix 1

Risk Classification

An incident (adverse event or near miss), complaint, claim or risk can all be classified according to the consequence or impact of the event or risk and the likelihood of it reoccurring or occurring in the first place.

Considering incidents and risks in this way enables such events to be graded into one of four categories: low, medium, high, and very high. Grading in this way determines the level of investigation and causal analysis that should be carried out. **NB INFORMATION GOVERNANCE INCIDENTS ARE SEPARATELY CLASSIFIED** (See appendix 2)

LIKELIHOOD			CONSEQUENCE or IMPACT				
	SCORES		Insignificant	Minor	Moderate	Severe	Catastrophic
			1	2	3	4	5
Rare	1		L	L	M	H	H
Unlikely	2		L	L	M	H	VH
Possible	3		L	M	H	VH	VH
Likely	4		M	H	H	VH	VH
Almost certain	5		H	H	VH	VH	VH

Green = low (L)
Yellow = medium (M)
Orange = high (H)
Red = very high (VH)

This risk classification system is adapted from the Risk Management Standard: AS/NZS 4360:1999.

Calculating the consequence

The consequence or impact of the risk or incident can be assessed and given a score using the following table as a guide. If a risk has several impacts then the highest one should be taken:

Type of consequence	Consequence Score				
	1	2	3	4	5
	Insignificant	Minor	Moderate	Severe	Catastrophic
Physical or psychological injury or illness	<ul style="list-style-type: none"> No visible injury or illness 	<ul style="list-style-type: none"> Minor injury or illness, requiring first aid treatment Grade 2 pressure sore Pain/distress 	<ul style="list-style-type: none"> RIDDOR Injury or illness requiring medical treatment (GP or A&E) Not-controlled infection Grade 3 pressure sore 	<ul style="list-style-type: none"> Injury/illness requiring acute hospital admission Permanent disability HSE prosecution Grade 4 pressure sore 	<ul style="list-style-type: none"> Unexpected death Serious multi-person adverse event Flu pandemic
Reputation	<ul style="list-style-type: none"> No impact on reputation 	<ul style="list-style-type: none"> Letters in local press 	<ul style="list-style-type: none"> Adverse article in local press Letters in national press Will result in one star being removed 	<ul style="list-style-type: none"> Adverse article in national press Will result in two stars being removed MP concern 	<ul style="list-style-type: none"> Will result in zero stars National media > 3days Adverse comments in the House
Performance	<ul style="list-style-type: none"> No impact on performance 	<ul style="list-style-type: none"> Failure to meet local targets 	<ul style="list-style-type: none"> Failure to meet national targets Failure to meet 1 key target 	<ul style="list-style-type: none"> Failure to meet developmental standards or other statutory requirements Failure to meet 2 key targets 	<ul style="list-style-type: none"> Failure to meet core standards Failure to meet 3 key targets
Financial	<ul style="list-style-type: none"> No financial loss 	<ul style="list-style-type: none"> 0-1% Directorate budget Theft/damage to personal property 	<ul style="list-style-type: none"> 1% Directorate budget 	<ul style="list-style-type: none"> 0-1% PCT budget 	<ul style="list-style-type: none"> >1% of PCT budget
Other		<ul style="list-style-type: none"> Minor breach of confidentiality* Brief verbal abuse 	<ul style="list-style-type: none"> Moderate breach of confidentiality* Minimal disruption of service Prolonged verbal abuse 	<ul style="list-style-type: none"> Verbal abuse with threatening behaviour Likely to result in tribunal Physical assault Patient abuse Serious breach of confidentiality* 	<ul style="list-style-type: none"> Extended disruption /closure of major service

* Please refer to guidance for Information Governance Incidents (Appendix 2)

The actual consequence or impact of a near miss will always be insignificant, and a near miss can never be classified as a serious untoward incident. However, a near miss can be an invaluable way of learning from an incident in which no harm, loss or damage occurred. It is therefore important to also consider the future risk of the incident occurring. To do this, the potential impact if a similar incident happening again must be assessed, along with the likelihood of it recurring. This will provide a risk score that will inform the level of investigation to be carried out.

Calculating the likelihood

This is the likelihood of occurrence or reoccurrence of the risk or event.

Level	Descriptor	Description
5	Almost certain	Is expected to occur/reoccur in most circumstances
4	Likely	Will probably occur/reoccur in most circumstances
3	Possible	Might occur/reoccur at some time
2	Unlikely	Could occur/reoccur at some time
1	Rare	May occur/reoccur only in exceptional circumstances

Appendix 2

Classification of Information Governance Incidents (SIRI)

The following process should be followed to categorise an IG SIRI

Step 1: Establish the scale of the incident. If this is not known it will be necessary to estimate the maximum potential scale point.

Baseline Scale (existing)

0	Information about less than 11 individuals
1	Information about 11-50 individuals
1	Information about 51-100 individuals
2	Information about 101-300 individuals
2	Information about 301 – 500 individuals
2	Information about 501 – 1,000 individuals
3	Information about 1,001 – 5,000 individuals
3	Information about 5,001 – 10,000 individuals
3	Information about 10,001 – 100,000 individuals
3	Information about 100,001 + individuals

Step 2: Identify which sensitivity characteristics may apply and the baseline scale point will adjust accordingly.

Low: For each of the following factors reduce the baseline score by 1 (-1 for each)
(A) No sensitive personal data (as defined by the Data Protection Act 1998) at risk nor data to which a duty of confidence is owed (B) Information readily accessible or already in the public domain or would be made available under access to information legislation e.g. Freedom of Information Act 2000 (C) Information unlikely to identify individual(s)
High: For each of the following factors increase the baseline score by 1 (+1 for each)
(D) Detailed information at risk e.g. clinical/care case notes, social care notes (E) High risk confidential information (F) One or more previous incidents of a similar type in the past 12 months (G) Failure to implement, enforce or follow appropriate organisational or technical safeguards to protect information (H) Likely to attract media interest and/or a complaint has been made directly to the ICO by a member of the public, another organisation or an individual (I) Individuals affected are likely to suffer substantial damage or distress, including significant embarrassment or detriment (J) Individuals affected are likely to have been placed at risk of or incurred physical harm or a clinical untoward incident

Cyber Sensitivity Factors

The following process should be followed to categorise a Cyber SIRI
Identify which sensitivity characteristics may apply and the baseline scale point will adjust accordingly.

Low: For each of the following factors reduce the baseline score by 1 (-1 for each)
(1) A tertiary system affected which is hosted on infrastructure outside health and social care networks.
High: For each of the following factors increase the baseline score by 1 (+1 for each)
(2) Repeat Incident (previous incident within last 3 months) (3) Critical business system unavailable for over 4 hours (4) Likely to attract media interest (5) Confidential information release (non-personal) (6) Require advice on additional controls to put in place to reduce reoccurrence (7) Aware that other organisations have been affected (8) Multiple attacks detected and blocked over a period of 1 month

Final Score	Level of SIRI
1 or less	Level 1 IG SIRI (Not Reportable to ICO)
2 or more	Level 2 IG SIRI (Reportable to ICO)

Appendix 3

Three levels of RCA investigation – guidance (NPSA)

Patient safety Root Cause Analysis (RCA) investigations should be conducted at a level appropriate and proportionate to the incident, claim, complaint or concern under review.

This document provides guidelines for what might be considered appropriate and proportionate.

Level 1 – Concise investigation

- Most commonly used for incidents, claims, complaints or concerns that resulted in no, low or moderate harm¹ to the patient.
- Also useful as an executive summary to communicate findings from full, comprehensive or independent investigation reports, following actual or potential 'severe harm or death' outcomes.
- Commonly involves completion of a summary or one page structured template.
- Includes the essentials of a thorough and credible investigation,² conducted in the briefest terms.
- Involves a select number of RCA tools (e.g. timeline, 5 why's, contributory factors framework).
- Conducted by one or more people (with a multidisciplinary approach if more than one investigator).
- Often conducted by staff local to the incident (ward/department/directorate/ GP surgery).
- Should include person(s) with knowledge of RCA, human error and effective solutions development.
- If a patient is directly affected, they/ relative/carer should be involved.
- Includes plans for shared learning – locally and/or nationally as appropriate.

Level 2 – Comprehensive investigation

- Commonly conducted for actual or potential 'severe harm or death'¹ outcomes from incidents, claims, complaints or concerns.
- Conducted to a high level of detail, including all elements of a thorough and credible investigation³
- Includes use of appropriate analytical tools (e.g. tabular timeline, contributory factors framework, change analysis, barrier analysis).
- Normally conducted by a multidisciplinary team, or involves experts/expert opinion/independent advice or specialist investigator(s).
- Conducted by staff not involved in the incident, locality or directorate in which it occurred.
- Overseen by a director level chair or facilitator.
- Led by person(s) experienced and/or trained in RCA, human error and effective solutions development.
- Includes patient/relative/carer involvement and should include an offer to patient/relative/carer of links to independent representation or advocacy services.
- May require management of the media via the organisation's communications department.
- Includes robust recommendations for shared learning, locally and/or nationally as appropriate.
- Includes a full report² with an executive summary and appendices.

Level 3 – Independent investigation

As per Level 2, but in addition:

- Must be *commissioned and conducted* by those independent to the provider service and organisation involved.
- Commonly considered for incidents, claims, complaints or concerns of high public interest or attracting media attention.
- Conducted for mental health homicides which meet Department of Health guidance.
- Should be conducted where Article 2 of the European Convention on Human Rights is, or is likely to be, engaged.

¹ As defined in the RCA Toolkit: www.npsa.nhs.uk/rcatoolkit

² As detailed in the 'RCA Investigation

³ Evaluation - thoroughness and credibility checklist' www.npsa.nhs.uk/rca

Appendix 4

RIDDOR Reportable incidents

Types of reportable incidents

Deaths and injuries

If someone has died or has been injured because of a work-related accident this may have to be reported. Not all accidents need to be reported, other than for certain [gas incidents](#), a RIDDOR report is required only when:

- the accident is [work-related](#)
- it results in an injury of a type which is reportable

Types of reportable injury

The death of any person

All deaths to workers and non-workers, with the exception of suicides, must be reported if they arise from a work-related accident, including an act of physical violence to a worker.

Specified injuries to workers

The list of 'specified injuries' in RIDDOR 2013 replaces the previous list of 'major injuries' in RIDDOR 1995. Specified injuries are (regulation 4):

- fractures, other than to fingers, thumbs and toes
- amputations
- any injury likely to lead to permanent loss of sight or reduction in sight
- any crush injury to the head or torso causing damage to the brain or internal organs
- serious burns (including scalding) which:
 - covers more than 10% of the body
 - causes significant damage to the eyes, respiratory system or other vital organs
- any scalping requiring hospital treatment
- any loss of consciousness caused by head injury or asphyxia
- any other injury arising from working in an enclosed space which:
 - leads to hypothermia or heat-induced illness
 - requires resuscitation or admittance to hospital for more than 24 hours

For further guidance on [specified injuries](#) is available.

Over-seven-day incapacitation of a worker

Accidents must be reported where they result in an employee or self-employed person being away from work, or unable to perform their normal work duties, for more than seven consecutive days as the result of their injury. This seven day period does not include the day of the accident, but does include weekends and rest days. The report must be made within 15 days of the accident.

Over-three-day incapacitation

Accidents must be recorded, but not reported where they result in a worker being incapacitated for more than three consecutive days. If you are an employer, who must keep an accident book under the Social Security (Claims and Payments) Regulations 1979, that record will be enough.

Non fatal accidents to non-workers (eg members of the public)

Accidents to members of the public or others who are not at work must be reported if they result in an injury and the person is taken directly from the scene of the accident to hospital for treatment to that injury. Examinations and diagnostic tests do not constitute 'treatment' in such circumstances.

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

If the accident occurred at a hospital, the report only needs to be made if the injury is a '[specified injury](#)' (see above).

Occupational diseases

Employers and self-employed people must report diagnoses of certain occupational diseases, where these are likely to have been caused or made worse by their work: These diseases include (regulations 8 and 9):

- carpal tunnel syndrome;
- severe cramp of the hand or forearm;
- occupational dermatitis;
- hand-arm vibration syndrome;
- occupational asthma;
- tendonitis or tenosynovitis of the hand or forearm;
- any occupational cancer;
- any disease attributed to an occupational exposure to a biological agent.

Further guidance on [occupational diseases](#) is available.



- Specific guidance is also available for: [occupational cancers](#)
- [diseases associated with biological agents](#)

Dangerous occurrences

Dangerous occurrences are certain, specified near-miss events. Not all such events require reporting. There are 27 categories of dangerous occurrences that are relevant to most workplaces, for example:

- the collapse, overturning or failure of load-bearing parts of lifts and lifting equipment;
- plant or equipment coming into contact with overhead power lines;
- the accidental release of any substance which could cause injury to any person.

Further guidance on these [dangerous occurrences](#) is available.

Additional categories of dangerous occurrences apply to [mines, quarries, offshore workplaces](#)  and relevant transport systems ([railways](#)  etc).

Gas incidents

Distributors, fillers, importers & suppliers of flammable gas must report incidents where someone has died, lost consciousness, or been taken to hospital for treatment to an injury arising in connection with that gas. Such incidents should be reported using the [online form](#).

Registered gas engineers (under the Gas Safe Register,) must provide details of any gas appliances or fittings that they consider to be dangerous, to such an extent that people could die, lose consciousness or require hospital treatment. The danger could be due to the design, construction, installation, modification or servicing of that appliance or fitting, which could cause:

- an accidental leakage of gas;
- incomplete combustion of gas or;
- inadequate removal of products of the combustion of gas.

Unsafe gas appliances and fittings should be reported using the [online form](#).

Appendix 5

Reporting of medication error incidents and adverse drug reactions

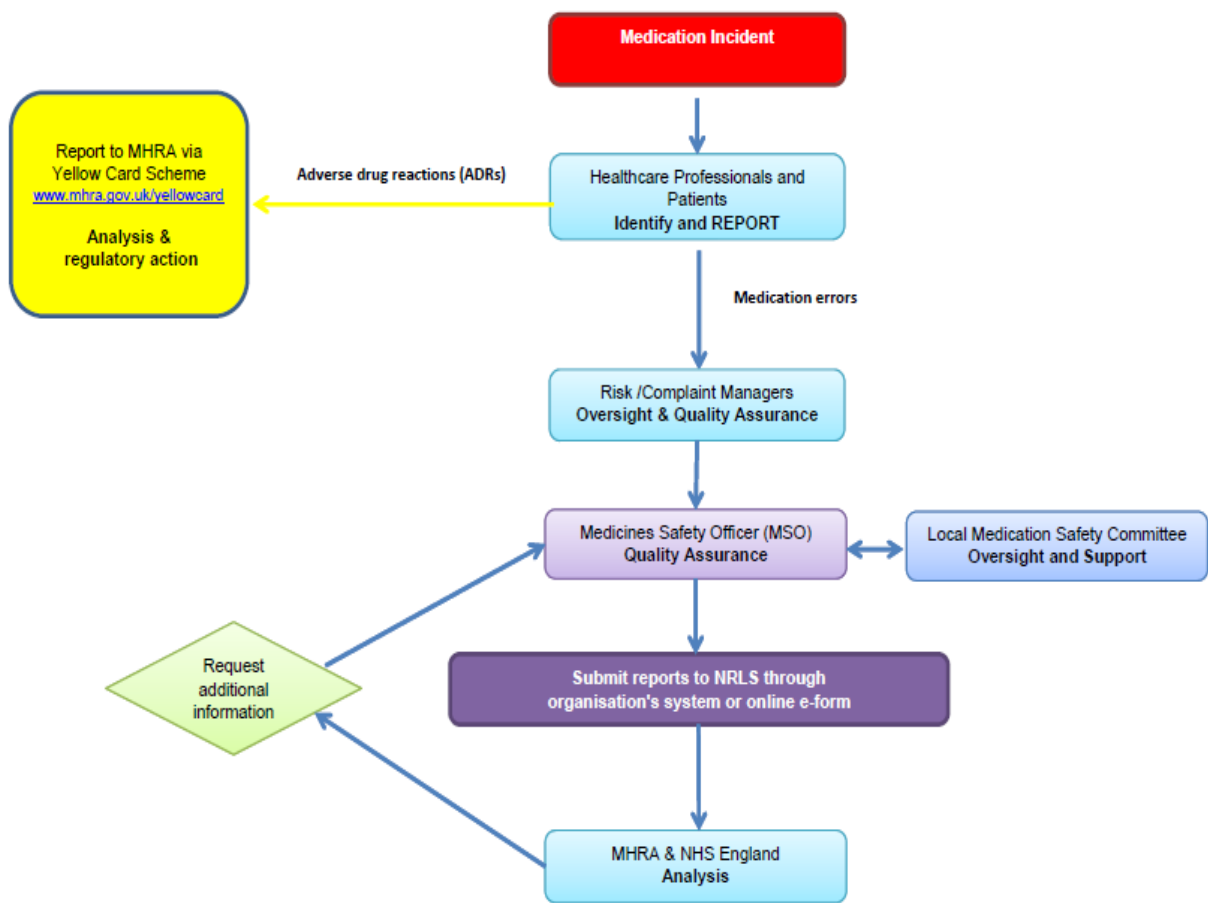
The system for reporting medication error incidents in England is the NRLS.

The MHRA and NHS England are working together to improve the quality and extent of reporting, and the resulting learning, in the field of medication errors. As part of this partnership, the NRLS will be an integrated reporting route for medication error incidents, see figure below.

Suspected ADRs not involving medication errors reported via the NRLS should continue to be sent directly to the MHRA through the Yellow Card Scheme. It is good practice to share copies of submitted Yellow Card reports with the MSO for local learning and action.

Near-miss incidents that have not caused harm but have the potential to do so and those involving errors of omission will stay in the NRLS and be used by the Patient Safety Domain in NHS England for national learning.

Improving reporting of medication incidents in the NHS



CONFIDENTIAL

INCIDENT REPORT FORM

REF NO:

Complete and Return to Leigh Broggi, Customer Care, Kingston Clinical Commissioning Group, Kingston, 3rd Floor Guildhall 1 Office, KT1 1EU (Email Leigh.Broggi@kingstonccg.nhs.uk) Tel: 0208-339-8107

THIS FORM SHOULD CONFIRM DETAILS OF FACT NOT OPINION. PLEASE PRINT CLEARLY

1. TYPE OF INCIDENT (please tick ONE box only)

- | | | |
|---|---|---|
| <input type="checkbox"/> Personal accident | <input type="checkbox"/> Clinical incident | <input type="checkbox"/> Business Continuity incident |
| <input type="checkbox"/> Corporate business incident | <input type="checkbox"/> Health & Safety incident | <input type="checkbox"/> Staff ill health incident |
| <input type="checkbox"/> Vehicle incident | <input type="checkbox"/> Fire incident | <input type="checkbox"/> Security, estates and environmental incident |
| <input type="checkbox"/> Information Governance/Breach of confidentiality | | <input type="checkbox"/> Violence/abuse/harassment |
| <input type="checkbox"/> Other, please specify | | |

2. DETAILS OF INCIDENT (state workplace or care area of person/property)

Directorate/Service Area etc:	<input type="text"/>	Date of Incident:	<input type="text"/>
Hospital/Clinic/Health Centre etc:	<input type="text"/>	Time of Incident: (24 hour clock)	<input type="text"/>
Ward/Dept/Unit etc: (if applicable)	<input type="text"/>	Exact Location: athroom)	<input type="text"/>

Description of what happened:

Immediate action taken to limit harm or damage and to prevent recurrence:

Using the KCCG Risk Management Matrix please indicate the actual severity/impact of this incident:

- ☐ Insignificant (no harm) ☐ Minor ☐ Moderate ☐ Severe ☐ Catastrophic
- You may need to consult your line manager to assist with this and also to consider whether a Root Cause Analysis (RCA) Investigation is appropriate. Please refer to the KCCG Incident Report Policy or the IG Reporting Guidance – from [HSCIC](#)

3. INCIDENT OUTCOME (please tick one box only, if more than one outcome then choose the main

- ☐ Disruption to services
- ☐ Breach of confidentiality
- ☐ Financial loss
- ☐ Other (please specify)
- ☐ Disruption to services
- ☐ Damage to property
- ☐ Damage/Loss of Assets
- ☐ Near miss by intervention (incident prevented)
- ☐Near miss (incident happened)

Other Consequences:
If Damage or Loss of Assets, please state costs involved:

4. NAME & ADDRESS (job title if staff) OF ANY WITNESSES (attach witness statements if

Full Name		Full Name	
Job Title		Job Title	
Address		Address	

5. THIS FORM HAS BEEN COMPLETED BY (please print clearly)

Refer to KCCG Incident Reporting Policy for further information. Follow HSCIC Serious Incident Reporting Incident Guidance if you consider that this incident may be an SIRI. Policies and guidance available on HCSIC

Completed by:Job Title:

Tel:

Workplace:Email:

Signature:Date:

6. THIS FORM MUST BE SIGNED OFF BY LINE MANAGER (please print clearly)

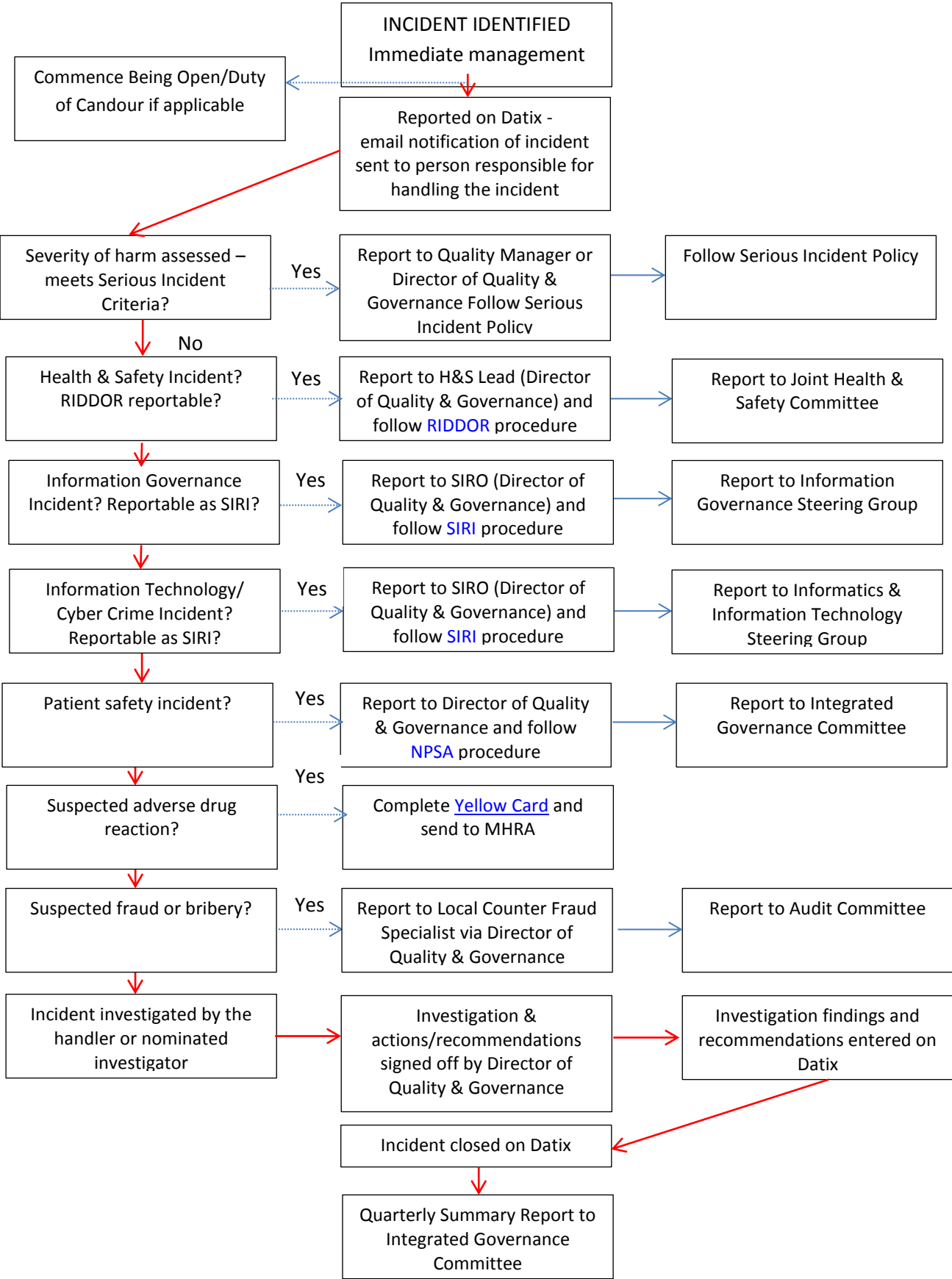
Please ensure you check all details, severity of the incident and action taken. You should keep copies of all incidents you sign off and investigate incidents in line with the KCCG Incident Policy and SIRI Guidance from HSCIC.

Name:Job Title:

Workplace:Email:

Signature:Date:

Appendix 7- Incident Management Flowchart



Appendix 8

Equality Impact Analysis					
Policy		Incident Management Policy			
Date of Analysis		8 th July 2016			
Completed by		Jill Pearse			
What are the aims and intended effects of the Policy		To ensure the CCG reports incidents in line with national requirements, takes appropriate action to learn from these and implements any actions to reduce the impact and reduce the risk of re-occurrence.			
Please list any other policies that are related to or referred to as part of this analysis?					
Who does the policy affect?		This policy applies to all staff working for, or on behalf of Kingston CCG.			
Equality Impact Analysis: Screening					
Characteristic	Could this policy have a positive impact based on		Could this policy have a negative impact based on		Comments
	Yes	No	Yes	No	
Race/ethnicity	X			X	Incidents may highlight issues relating to race or ethnicity -Implementing learning from any such incidents is likely to promote equality
Age	X			X	Incidents may highlight issues relating to age-Implementing learning from any such incidents is likely to promote equality
Disability	X			X	Incidents may highlight issues relating to disability -Implementing learning from any such incidents is likely to promote equality
Gender	X			X	Incidents may highlight issues relating to gender-Implementing learning from any such incidents is likely to promote equality
Gender reassignment	X			X	Incidents may highlight issues relating to gender reassignment-Implementing learning from any such incidents is likely to promote equality
Pregnancy and Maternity	X			X	Incidents may highlight issues relating to pregnancy and maternity-Implementing learning from any such incidents is likely to promote equality
Marital Status	X			X	Incidents may highlight issues relating to marital status -Implementing learning from any such incidents is likely to promote equality
Religion or Belief	X			X	Incidents may highlight issues relating to religion or belief-Implementing learning from any such incidents is likely to promote equality
Sexual orientation	X			X	Incidents may highlight issues relating to sexual orientation-Implementing learning from any such incidents is likely to promote equality