NHS
Bury
Clinical Commissioning Group

Data Security & Protection Breaches / Information Governance Incident Reporting Policy and Procedure

Version:	5.0
Ratified by:	NHS Bury Clinical Commissioning Group Information Governance Operational Group
Date ratified:	31st October 2018
Name of originator /author (s):	Information Governance Team
Responsible Committee / individual:	NHS Bury Clinical Commissioning Group Audit Committee
Date issued:	November 2018
Review date:	November 2020
Target audience:	NHS Bury Clinical Commissioning Group Members and Staff
Equality Analysis Assessed:	Yes

Further information regarding this document

Document name	Data Security & Protection Breaches / Information Governance Incident Reporting Policy CCG.GOV.020.5.0
Category of Document in The Policy Schedule	Governance
Author(s) Contact(s) for further information about this document	Information Governance Team
This document should be read in conjunction with	Information Governance Policy; Records Management Policy; Information Risk Policy; Freedom of Information Policy; Acceptable Use Policy; Confidentiality Guidelines for staff; Secure Transfer of Data Procedure.
This document has been developed in consultation with	NHS Bury Clinical Commissioning Group Information Governance Operational Group
Published by	NHS Bury Clinical Commissioning Group 1 Knowsley Place Knowsley Street Bury BL9 0SN Main Telephone Number: 0161 762 1500
Copies of this document are available from	CCG Corporate Office CCG website

Version Control

Version History:		
Version Number	Reviewing Committee / Officer	Date
3.0 = policy once ratified	NHS Bury Clinical Commissioning Group, Quality and Risk Committee	15th February 2016
3.1 = policy once reviewed	GMSS IG Team	8th November 2017
4.0 = policy once ratified	NHS Bury Clinical Commissioning Group Information Governance Operational Group	29th November 2017
4.1 = policy once reviewed	GMSS IG Team	24th September 2018
5.0 = policy once ratified	NHS Bury Clinical Commissioning Group Information Governance Operational Group	31st October 2018

Data Security & Protection Breaches / Information Governance Incident Reporting Policy and Procedure

Table of Contents

1. Introduction

NHS Bury Clinical Commissioning Group (hereafter referred to as the CCG) is committed to a programme of effective risk and incident management. The CCG has a responsibility to ensure data breaches and / or information governance incidents are reported and managed efficiently and effectively.

The General Data Protection Regulation (GDPR) brought in in May 2018 requires that where personal data breaches affect the 'rights and freedoms of an individual,' Article 33 (of GDPR) imposes a duty to report these types of personal data breach to NHS Digital and to the Information Commissioner's Office (ICO). In some cases, these will also be reported to Department of Health and Social Care (DHSC). These are reported using the Incident Reporting Tool housed in the Data Security and Protection Toolkit (DSPT).

This procedure explains the system to be used for staff for the recording, reporting and reviewing data security and protection breaches / incidents. This supports the CCG's overall incident reporting process which is an integral part of personal, clinical and corporate governance.

The information contained within this procedure is taken from the "Guide to the Notification of Data Security and Protection Incidents" produced by NHS Digital (May 2018). Further detailed information about data breach reporting can be found in this document and must be referred to when reading this procedure and grading any personal data breach / incident. The guidance can be found on the following link:

https://www.dsptoolkit.nhs.uk/Help/29

It is a contractual requirement to include statistics on personal data breaches in the annual report and the Statement of Internal Control (SIC) presented to the Board and the CCG must keep a record of any personal data breaches, regardless of whether it is required to notify these to the ICO. The Information Governance (IG) Team co-ordinate and maintain a Data Security Breaches / Incident Reporting Logbook.

The CCG is not subject to the Security of Network Information Systems (NIS) Regulations 2018 and is therefore not required to report breaches under this regulation.

2. Purpose

This document sets out the directions across the CCG for the reporting and management of Data Security & Protection breaches / incidents.

For those staff covered by a letter of authority / honorary contract or work experience the organisation's policies are also applicable whilst undertaking duties for or on behalf of the CCG.

Further, this procedure applies to all third parties and others authorised to undertake work / process data on behalf of the CCG.

3. Definitions

Personal Data Breach

As per Article 4(12) of the GDPR, a "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.

The traditional view that a personal 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. These types of breaches are graded as per the guidance from NHS Digital using a risk scoring 5x5 matrix and maybe notifiable to the Information Commissioners Office (ICO) if they attain a grade as described in the guidance.

Personal data

This is data defined as any information relating to an identified or identifiable living individual.' An "Identifiable living individual" means a living individual who can be identified, directly or indirectly, 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.

All paper records that relate to a living individual and any aspect of digital processing such as IP address and cookies are deemed personal data. GDPR also introduces geographical data and biometric data to be classified as personal data.

Special Categories of Personal Data

Under GDPR, these are:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- the processing of genetic data
- biometric data for uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation

For data security breach reporting purposes, special categories of data also 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

Breach Types

The Article 29 working party, an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission now known as the European Data Protection Board (EDPB) under the EU General Data Protection Regulation (GDPR) from 25th May 2018 categorised data security breaches into 3 categories which were associated with confidentiality, integrity and / or availability.

The CIA Triad

A definition of each category of breach is detailed below:

- Confidentiality Breach – Unauthorised or accidental disclosure of, or access to personal data
- Availability Breach – Unauthorised or accidental loss of access to, destruction of personal data
- Integrity Breach – Unauthorised or accidental alteration of personal data

Table 1 below states the ICO categorisation of data breaches in conjunction with the type of breach category as identified by the Article 29 Working Party.

Please note further details regarding the types of breaches under each of the CIA Triad can be found in the "Guide to the Notification of Data Security and Protection Incidents" guidance document.

Table 1 – ICO and Article 29 Working Group classification of data security breaches

	ICO Categorisation	Type of Breach (Art 29 Working Party)
A	Data sent by email to incorrect recipient	Confidentiality
B	Cyber security misconfiguration (e.g. inadvertent publishing of data on website; default passwords)	Confidentiality
C	Cyber incident (phishing)	Confidentiality
D	Insecure webpage (including hacking)	Confidentiality

	ICO Categorisation	Type of Breach (Art 29 Working Party)
E	Cyber incident (key logging software)	Confidentiality
F	Loss or theft of paperwork	Availability
G	Loss or theft of unencrypted device	Availability
H	Loss/theft of only copy of encrypted data	Availability
I	Data left in insecure location	Availability
J	Cyber incident (other - DDOS etc.)	Availability
K	Cyber incident (exfiltration)	Availability
L	Cryptographic flaws (e.g. failure to use HTTPS; weak encryption)	Availability
M	Insecure disposal of paperwork	Availability
N	Insecure disposal of hardware	Availability
O	Other principle 7 failure	Integrity
P	Cyber incident - unknown	Integrity

4. Roles and Responsibilities

Chief Operating Officer

Has ultimate responsibility for the implementation of the provisions of this policy and procedure. As the 'Accountable Officer' they are responsible for the management of the organisation and for ensuring that the appropriate mechanisms are in place to support incident reporting for Data Security and Protection incidents. .

Data Protection Officer (DPO)

This is a new role required as per the General Data Protection Regulations (GDPR). The DPO's role is to inform and advise the CCG and its staff about their obligations to comply with the GDPR and other current data protection laws. They are required to monitor compliance with the GDPR and current data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits. In addition they are required to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

For the purposes of incident reporting the DPO will provide advice and guidance around the grading and categorisation of any Data Security and Protection Incident, and in the event of a reportable incident to the ICO, will be the point of contact.

Caldicott Guardian

To review and provide feedback regarding an incident where this relates to patient data. This may involve decision making about informing patients regarding an incident or not if this would deem to cause them harm / distress.

Senior Information Risk Owner (SIRO)

To review data security and protection incidents and report issues to the Audit Committee and Senior Management Team and ensure that any external reporting of the incident if required is undertaken

Information Governance Team

Has responsibility to:

- To co-ordinate and investigate reported data and security protection incidents, maintain the CCG Incident / Data and Security Breaches Reporting Logbook, make recommendations and act on lessons learnt.
- To liaise with the CCG IG Lead, CCG SIRO and Greater Manchester Shared Services (GMSS) IT Services / IT Security Lead and CCG IT Manager as appropriate pertaining to data security incidents.
- To escalate incidents to the CCG IG Lead in order to inform the SIRO, DPO, Caldicott Guardian as appropriate.
- To grade the incident and report it where necessary on the Data and Security Breaches Reporting Toolkit Incident Reporting Tool and local CCG IG Incident / Data Breaches Logbook.

CCG IT Manager

- To work with GMSS IT and the IT Security Manager to investigate the incidents where IT and IT Security input is required, make recommendations and act on lessons learnt.
- To liaise with IG Teams as appropriate especially regarding reporting.
- To inform the Senior Information Risk Owner, DPO, Caldicott Guardian as appropriate.

GMSS IT Services / IT Security Manager

To alert the CCG IT Lead, IT Security Manager and IG Team when a member of CCG staff reports a potential or actual information security incident / IT / cyber security incident that is reportable as per the NHS Digital process via the IT Service Desk. This can then be investigated, reported and graded accordingly on the Data Breaches / Incident Reporting Logbook and the DSPT Incident Reporting Tool if this requires escalation and reporting to the ICO / NHS Digital.

Line Managers

Line managers are responsible for ensuring that all staff, particularly new staff, temporary staff, contractors and volunteers, know what is expected of them with respect to reporting data security & protection breaches / incidents.

CCG Employees

Staff and members are responsible for maintaining the confidentiality of all personal and corporate information gained during their employment term of office with the CCG and this extends after they have left the CCG.

5. Data Security Breaches / Incident Investigation Process

All data security breaches / incidents must be reported to the CCG IG Lead / DPO / IG Team AS SOON AS THIS INCIDENT IS KNOWN following the CCG's incident reporting processes (detailed below). Staff should not delay the reporting of any incident even if unsure whether it may not be a breach / incident. If it is identified as a data security breach / incident, it will be logged on the CCG Data Security Beaches / Incident Reporting Logbook. The CCG Lead / SIRO / Caldicott Guardian / DPO and IG Team will assess the incident using the NHS Digital's guidance to grade it accordingly.

The CCG will continue to utilise its own internal incident reporting procedure for the management of incidents. All incidents must be reported initially to the CCG IG Lead and IG Team.
The immediate response to an incident and the escalation process for investigation or external reporting will vary according to the severity level of the incident.

Where incidents are identified as a Data Security / IG incident the CCG IG Lead and IG Team will liaise and the DPO.

The IG Team will log this on the local CCG Data Security Breach / Incident Reporting Logbook and assess and grade using the Breach Assessment Guide (Appendix 2).

Incident Grading

Incidents are graded according to the significance of the breach on a scale of 1-5 (1 being the lowest and 5 being the highest) and the likelihood of those serious consequences occurring on a scale of 1-5 (1 being the lowest and 5 being the highest). Please note incident / breaches are graded according to the impact on the individuals it concerns and not the organisation.

Article 34 requires the CCG to notify the relevant authority when an incident constitutes a high risk to the rights and freedoms of an individual. This is classified when a breach 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

The tables in Appendix 1 set out how to grade the severity of a personal data breach / incident to see if it is high risk and be significant enough to be reported to the ICO. The Breach Assessment Grid in Appendix 2 ascertains when an incident is notifiable and to whom.

When incidents are notifiable, this is carried out using the NHS Digital Incident Reporting Tool housed in the Data Security and Protection Toolkit (DSPT).

Vulnerable Groups

Where a data security breach relates to a vulnerable group in society, a minimum risk assessment score of 2 for likelihood and significance is stated unless the incident has been contained.

Time scale for reporting

Article 33 of GDPR requires reporting of a breach within 72 hours. This is from when the CCG becomes aware of the breach and may not be necessarily when it occurred. However, it is important that all staff report any IG incidents / breaches AS SOON AS POSSIBLE. Failure to notify promptly may result in action taken by the ICO by breaching Article 33.

It is mandatory for all staff to report 'near misses' as well as actual incidents, so that we can take the opportunity to identify and disseminate any 'lessons learnt'.

Informing the public

Article 34 requires that the public are notified if a data security breach results in a high risk to the rights and freedoms of individuals. In summary, this notification must include a description of the breach, name and contact details of the DPO or equivalent, a description of the likely consequences of the breach and a description of the measures taken or to be taken to address and mitigate the breach and its possible adverse effects.

If the CCG does not decide to notify individuals it must have a justified reason to demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of individuals it concerns.

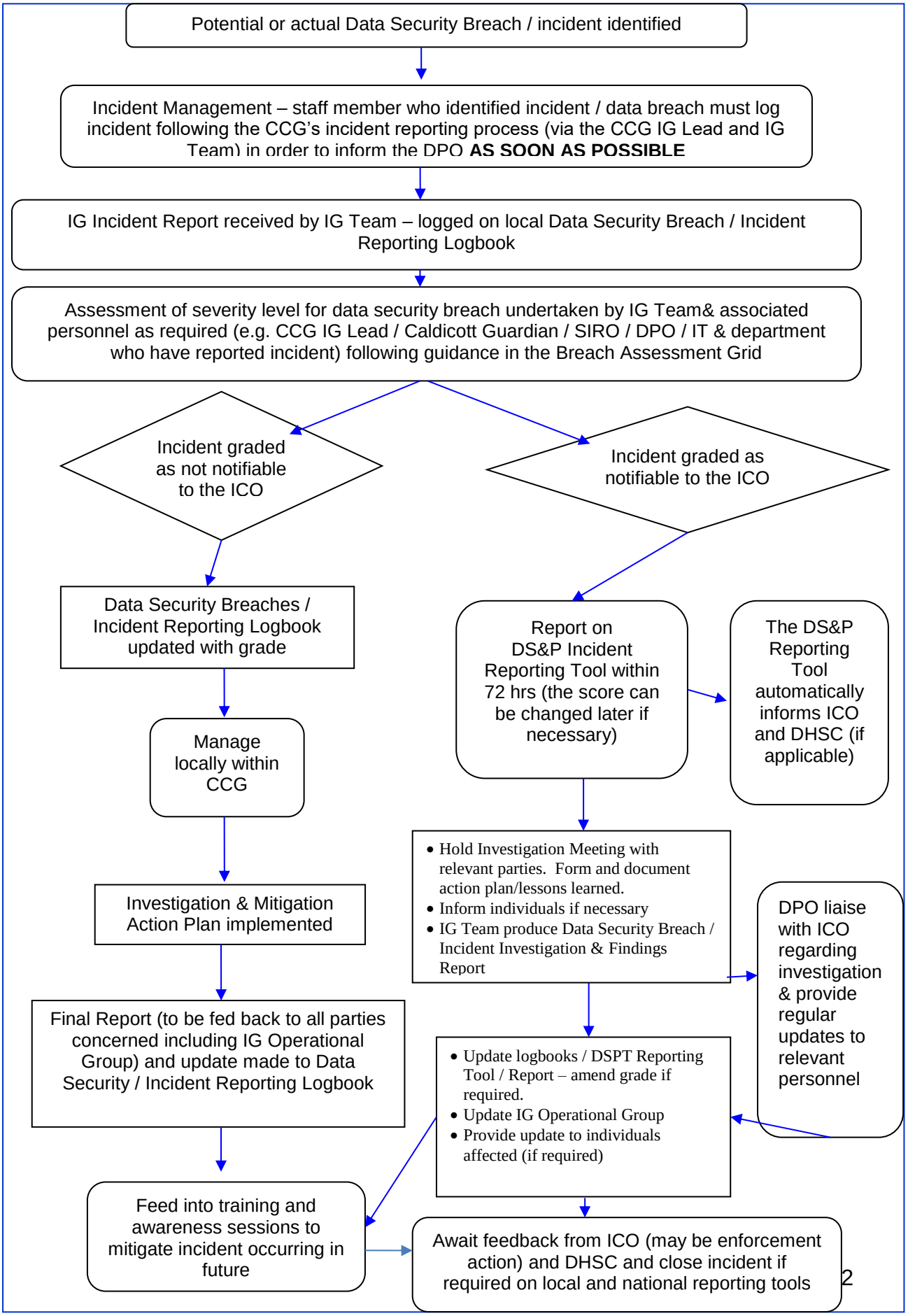
Containment Actions which affect notification status

There may be circumstances where the CCG is aware of a breach but there are containment actions that remove the need for notification to the ICO but will still be recorded locally. For example, notification may not be necessary when:

- Encryption is used to protect personal data
- Where personal data is recovered from a trusted partner organisation. A trusted partner is classified when the controller (CCG) may have a level of assurance with the recipient so that it can reasonably expect that party not to read or access the data sent in error and to comply with instructions to return it. Even if the data has been accessed, the CCG could still possibly trust the recipient not to take any further action and return and co-operate with the CCG's instructions
- Where the CCG can null the effect of any personal data breach

The flowchart (Figure 1) sets out the overall process for reporting, managing and investigating data security and protection incidents / personal data breaches for the CCG.

Figure 1 – Data Security Breach / Incident Reporting Flowchart



6. Reporting

Reporting in the Annual Governance Statement / Statement of Internal Control

Reportable incidents that affect the rights and freedoms of an individual need to be detailed in the annual report / governance statement / Statement of Internal Control as outlined in Table 1 below.

Table 1 - Summary of Data Security and Projection Incidents reported to the ICO and/or Department of Health and Social Care (DHSC)

Date of incident (month)	Nature of incident	Number affected	How patients were informed	Lesson learned

Reporting by NHS Digital

Data breaches reported via the DSPT Incident Reporting Tool will be forwarded to the appropriate organisation indicated in the guidance such as the Department of Health and Social Care (DHSC), NHS England and the ICO. Additionally, these organisations may have obligations to work with other agencies, such as the National Cyber Security Centre, for example, and any incident information may be shared onward. For this reason, it is prohibited to include individual information that could identify any person affected by a breach. All incidents will be shared on a quarterly basis in aggregate form for incident monitoring and trend analysis.

Reporting to the CCG's Audit Committee

Data Security breaches / incidents are reported routinely at the CCG's Information Governance Operational Group (via the IG Key Statistics Report) who report to the CCG's Audit Committee. Lessons learned are discussed and actioned when necessary to assist mitigation of future similar incidents.

7. Closure and Lessons Learned

It is essential that action is taken to help to minimise the risk of data breaches / IG incidents re-occurring in the future. Therefore, all data breaches / IG incidents that are reported will be logged and any associated lessons learned will be fed back to staff. This may be communicated via email / staff briefings / team meetings.

Staff involved with a data breach / IG incident should consider with their line manager if additional training and support is needed. The investigation team and / or IG Team will determine this. Line managers should contact the IG Team for further assistance.

8. Training and Awareness

Line managers are responsible for ensuring that all staff, particularly new staff, temporary staff, contractors and volunteers, know what is expected of them with respect to confidentiality and protecting information. They are also responsible for monitoring compliance with this guideline e.g. undertake ad hoc audits to check for inappropriate disclosures, records left out, abuse of passwords etc.

Staff are responsible for maintaining the confidentiality of all personal and corporate information gained during their employment with the CCG and this extends after they have left the employ of the CCG.

Individual staff members are personally responsible for any decision to pass on information that they may make.

All staff are responsible for adhering to the Caldicott Principles, the Data Protection Act 2018, General Data Protection Regulation, the Confidentiality Code of Conduct, the National Data Guardian Security Standards and the common law duty of confidentiality.

Staff will receive instruction and direction regarding the policy from a number of sources:

- Policy /strategy and procedure manuals; line manager;
- specific training course;
- other communication methods (e.g. team brief/team meetings); staff Intranet;

All staff are mandated to undertake Data Security / Information Governance training on an annual basis. This training should be provided within the first year of employment and then updated as appropriate in accordance with the Information Governance policy.

9. Monitoring and review

This procedure will be reviewed every two years, and in accordance with the following on an as and when required basis:

- legislative changes; good practice guidance; case law;
- significant incidents reported; new vulnerabilities; and
- changes to organisational infrastructure.

10. Legislation and related documents

A set of procedural document manuals will be available via the CCG's website.

Staff will be made aware of procedural document updates as they occur via team briefs, team meetings and notification via the CCG staff Intranet.

A number of other policies are related to this policy and all employees should be aware of the full range below:

- Information Governance Framework
- Information Governance Policy
- Data Protection and Confidentiality Policy
- Information Security Policy
- Acceptable Use Policy
- Records Management Policy
- Information Risk Policy
- Confidentiality Audit Policy
- Information Security Policy

Acts Covered Under Policy

- General Data Protection Regulation
- Data Protection Act 2018

Appendix 1 - Guide to Notification of Data Security & Protection Incidents

Establish the likelihood that adverse effect has occurred:

No.	Likelihood	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

If the likelihood that an adverse effect has occurred is low and the incident is not reportable to the ICO, no further details will be required.

Grade the potential severity of the adverse effect on individuals:

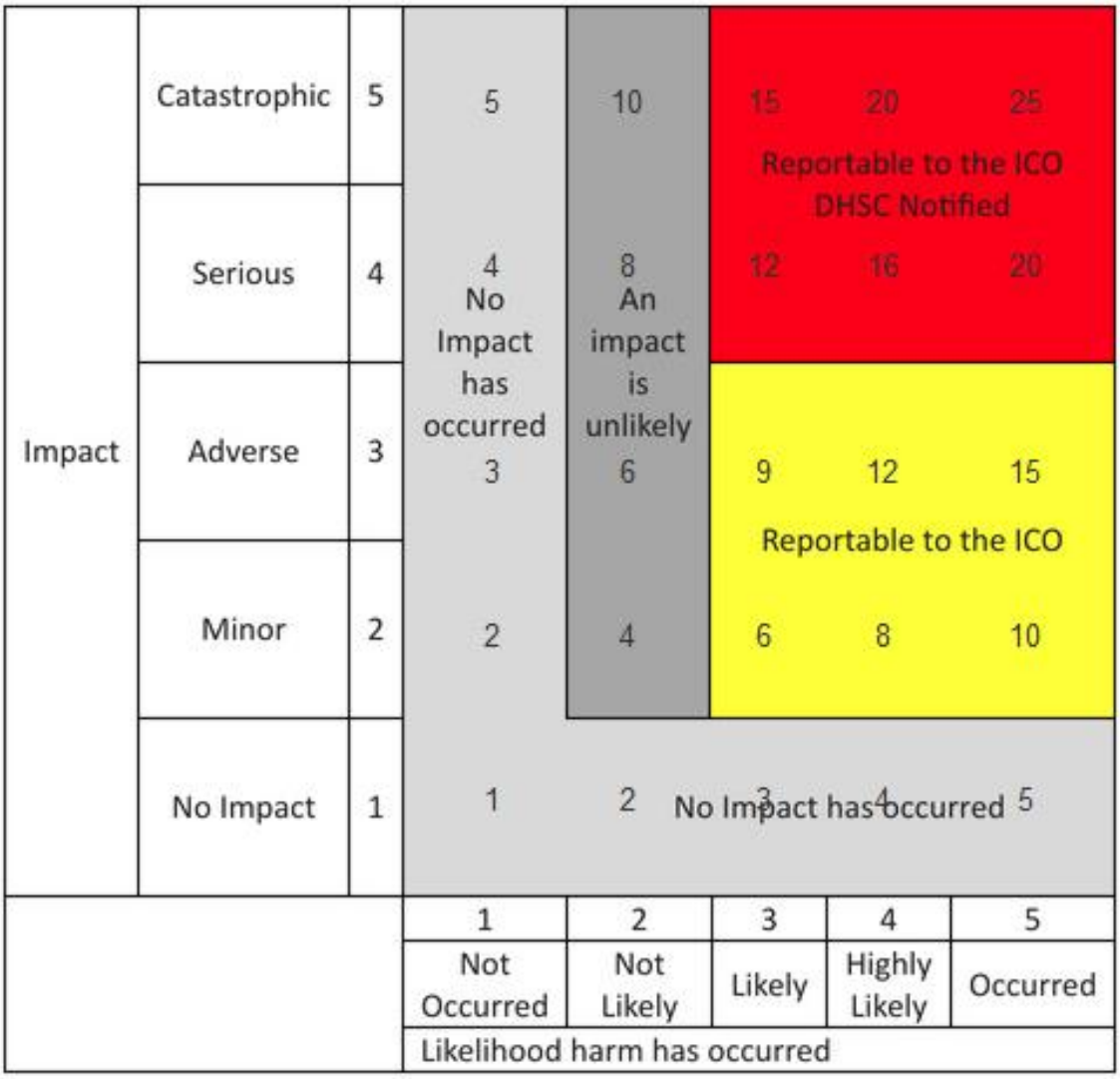
No.	Effect	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.
3	Potentially some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.
4	Potentially Pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence

Both the adverse effect and likelihood values form part of the breach assessment grid.

Appendix 2 – Breach Assessment Grid

This operates on a 5 x 5 basis with anything other than “grey breaches” being reportable / notifiable to the ICO / DHSC via the DSPT incident reporting tool.

Incidents where the grading results are in the red are advised to be notified within 24 hours.



Appendix 3 - Key Contacts

CCG Information Governance Team:

Caldicott Guardian - Dr Jeff Schryer
Email: **jeffrey.schryer@nhs.net**

Senior Information Risk Owner (SIRO) – Mike Woodhead
Email: **mike.woodhead@nhs.net**

CCG IG Lead – Emma Kennett
Email: **emma.kennett@nhs.net**

CCG IT Lead – Mike Culshaw
Email: **mikeculshaw@nhs.net**

GMSS IG Team:
Caroline Cross – IG Manager
Email: **caroline.cross@nhs.net**

Camilla Bhondoo – Senior IG Officer
Email: **Camilla.bhondoo@nhs.net**