NHS

Walsall Clinical Commissioning Group

Data Breach Policy and Procedure

Data Breach Policy and Procedure
For
Walsall Clinical Commissioning Group

The Audit & Governance Committee approved this document on:

Date: 05 March 2019
Signed: Chair of the committee
Signed: Designated Senior Officer

Please note that the Intranet version of this document is the only version that is maintained. Any printed versions should therefore be viewed as 'uncontrolled' and may not be the most up-to-date.

Version:	**V1.0**
Status	Ratified
CCG Lead	Head of Corporate Governance, Sara Saville
Senior Officer responsible	Chief Officer, Simon Brake
Ratified by:	Audit & Governance Committee
Date ratified:	05 March 2019
Date Policy is Effective From	Date of ratification
Review date:	January 2020
Expiry date:	March 2020
Date of Equality and Diversity Impact Assessment	
Date of Health Inequalities Impact Assessment	
Target audience:	CCG staff and staff working for the CCG
National Documents	
CCG linked documents	
Distribution of the document	Hard copies available at reception, accessible from Website, IG team and IG Newsletter.
Implementation of the document	
Document Control and Archiving	Obsolete or superseded documents will be removed from the intranet and where relevant replaced with an updated version. Previous versions will be archived in the safeguard system in accordance with the Records Management NHS Code of Practice; disposal and retention schedule.
Monitoring Compliance and Effectiveness	
References	

CONTRIBUTION LIST
Key individuals involved in developing the document

Name	Designation

Circulated to the following for consultation

Name/Committee/Group/	Designation

IG Function Leads	
Audit & Governance Committee	

Comments received from consultation

Name/Committee/Group	Comments

Version Control Summary

Significant or Substantive Changes from Previous Version

Version	Date	Comments on Changes	Author

Contents

1. Introduction

Walsall Clinical Commissioning Group has a responsibility to ensure data breaches and/or information governance incidents are reported and managed efficiently and effectively. Where personal data breaches affect the 'rights and freedoms of an individual, GDPR (Article 33) 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). This are reported using the Incident Reporting Tool housed in the Data Security and Protection Toolkit (DSPT).

The protection and security of the data that we hold and use, including personal information, is paramount to us and we have developed data specific controls and protocols for any breaches involving personal information and data subject to the GDPR requirements.

2. Scope

This procedure describes the process for staff to follow regarding recording, reporting and reviewing of data security and protection breaches and 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 Governing Body 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 Corporate Governance Officer maintains a Data Security Breaches/Incident Reporting Logbook.

3. Purpose

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

This procedure applies to all staff within the CCG, and to ensure that the CCG is meeting its legal, statutory and regulatory requirements under the General Data Protection Regulation and to ensure that all personal and special category information is safe, secure and processed compliantly.

4. Definitions

4.1 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.

4.2 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.

4.3 Special Categories of Personal Data

Under GDPR, these are:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- and 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:

4.4 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

5. Breach Types

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.

	ICO Categorisation	**Type of Breach (Article 29 Working Party)**
A	Data sent by email to incorrect recipient	Confidentiality
B	Data posted or faxed to incorrect recipient	Confidentiality
C	Failure to redact data	Confidentiality
D	Information uploaded to webpage	Confidentiality
E	Verbal reasoning	Confidentiality
F	Failure to use bcc when sending email	Confidentiality
G	Cyber Security misconfiguration (e.g. inadvertent publishing of data on website; default passwords	Confidentiality
H	Cyber incident (phishing)	Confidentiality
I	Insecure webpage (including hacking)	Confidentiality
J	Cyber incident (key logging software)	Confidentiality
K	Loss or theft of paperwork	Availability
L	Loss or theft of unencrypted	Availability

	device	
M	Loss/theft of only copy of encrypted data	Availability
N	Data left in insecure location	Availability
O	Cyber incident (other - DDOS etc.)	Availability
P	Cyber incident (exfiltration)	Availability
Q	Cryptographic flaws (e.g. failure to use HTTPS; weak encryption)	Availability
R	Insecure disposal of paperwork	Availability
S	Insecure disposal of hardware	Availability
T	Other principle 7 failure	Integrity
U	Cyber incident - unknown	Integrity

6. Objectives

- To adhere to the GDPR and UK Data Protection laws and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any data breaches
- To develop and implement adequate, effective and appropriate technical and organisational measures to ensure a high level of security with regards to personal information
- To utilise information audits and risk assessments for mapping data and reducing the risk of breaches
- To have adequate and effective risk management procedures for assessing any risks presented by processing personal information
- To ensure that any data breaches are reported to the correct regulatory bodies within the timeframes as set out in their code of practice or handbooks
- To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring
- To use the Data Breach Incident Form for all data breaches, regardless of severity so that any patterns in causes can be identified and corrected
- To protect patients and staff – including their data, information and identity
- To ensure that where applicable, the Data Protection Officer is involved in and notified about all data breaches and risk issues
- To ensure that the Supervisory Authority is notified of the data breach (where applicable) with immediate effect and at the latest, within 72 hours after having become aware of the breach

7. Roles and responsibilities

7.1 Chief Officer

The Chief Officer is the lead on the Governing Body for Information Governance.

7.2 Chief Financial Officer (Senior Information Risk Owner)

The CCGs Chief financial officer is the Senior Information Risk Owner (SIRO). The role of the SIRO is to take ownership of the organisations information risk policy, act as an advocate for information risk on the Governing Body and provide written advice to the Accountable Officer on the content of the annual governance statement in regard to information risk.

7.3 Medical Director (Caldicott Guardian)

Responsibility for ensuring that all patient related personal data is processed and managed in accordance with the Caldicott Principles. The Medical Director acts as the CCGs Caldicott Guardian with responsibility for patient confidentiality.

7.4 Data Protection Officer

The CCG have appointed a Data Protection Officer (DPO) whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up-to-date with all legislation and changes relating to data protection.

The DPO will work in conjunction with others to ensure that all processes, systems and staff are operating compliantly and within the requirements of the GDPR and its principles.

The DPO has overall responsibility for due diligence, Data Protection Impact Assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the GDPR and our own internal objectives and obligations.

The Data Protection Officer has assumed the below duties in compliance with GDPR Article 39: -

- To inform and advise the CCG and any employees carrying out processing, of their obligations pursuant to the GDPR, the Supervisory Authorities guidelines and any associated data protection provisions
- To monitor compliance with the GDPR, associated data protection provisions and THE CCGs own data protection policies, procedures and objectives
- To oversee the assignment of responsibilities, awareness-raising and training of staff involved in processing operations
- To carry out and review audits of the above-mentioned policies, procedures, employee duties and training program
- To co-operate with the Supervisory Authority where required

- To act as the point of contact for the Supervisory Authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter
- In accordance with Article 35 (type of processing is likely to result in a high risk to the rights and freedoms of natural persons), the DPO will provide advice where requested with regards to any data protection impact assessment and monitor its performance pursuant
- Have due regard to, and be aware of, the risk associated with processing operations, considering the nature, scope, context and purposes of processing
- The above-mentioned policies, procedures, employee duties and training programs

Name: Curtiss Green, GR Governance & Consultancy
Email: dataprotection.officers@nhs.net

7.5 Corporate Governance Lead

Responsibility for ensuring there are information governance arrangements in place to allow for the processes laid out within this policy and procedure.

7.6 Information Governance Operational Group

The Information Governance Operational Group IGOG purpose is to support and drive the broader information governance agenda. The group will make recommendations to the Audit & Governance Committee and provide assurance that the CCG is compliant with IG requirements.

7.7 All Staff

All staff must ensure they understand and adhere to the requirements of this policy.

8. Data Security Breaches / Incident Investigation Process

Staff must follow the CCG's process for incident reporting which includes any data security breaches or incidents. All data security breaches and incidents must be reported initially to the CCG IG Lead AS SOON AS THIS INCIDENT IS KNOWN following the CCG's incident reporting processes. Please do not delay reporting of any incident even if you suspect it may not be an incident or breach. If it is identified as a data security breach or incident, it will be logged on the CCG Data Security Beaches / Incident Reporting Logbook. The IG Lead, SIRO, Caldicott Guardian and DPO will assess the incident using the NHS Digital's guidance to grade it accordingly.

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 B sets 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 B ascertains when an incident is notifiable and to whom.

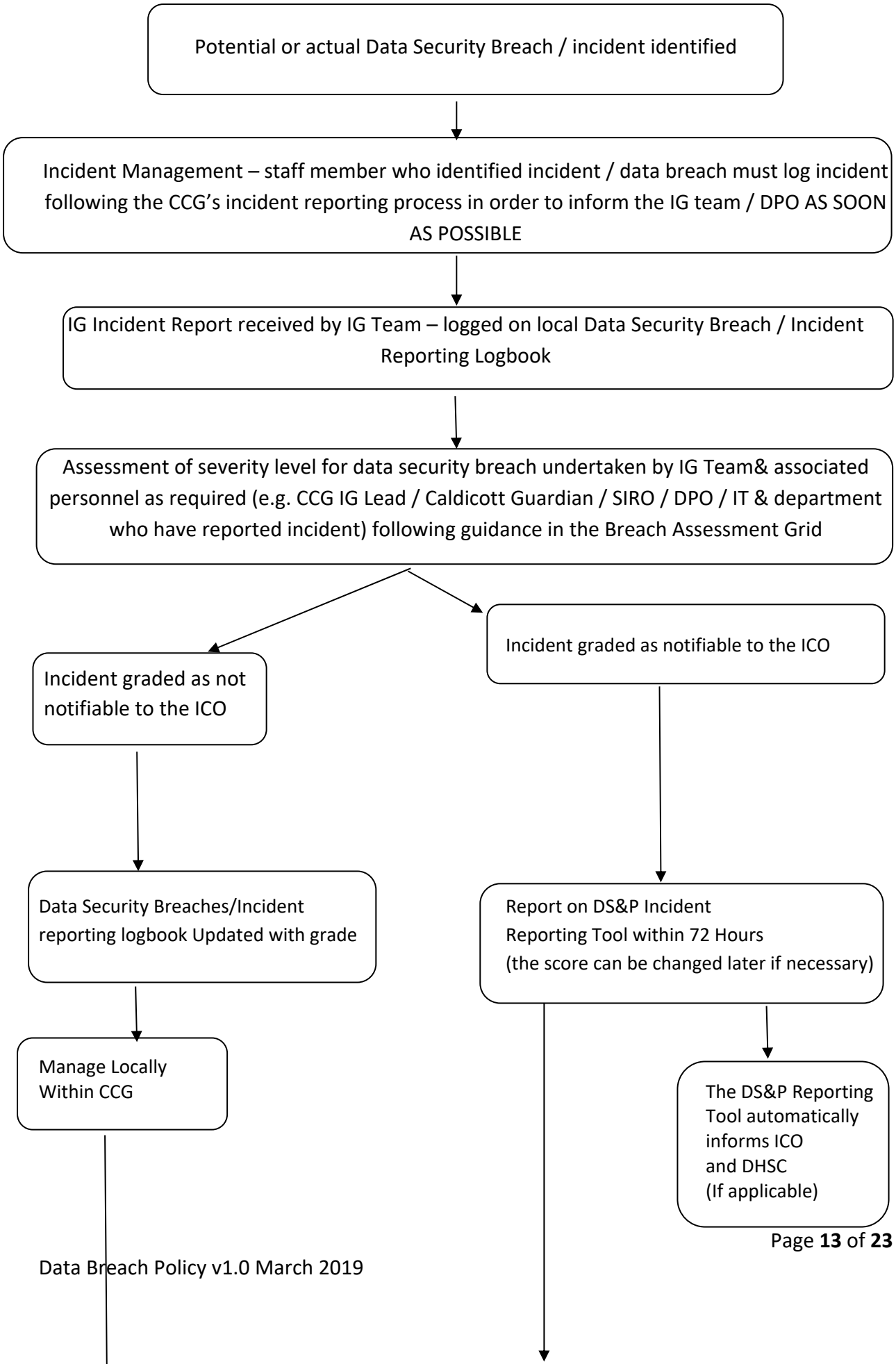
When incidents are notifiable, this is carried out using the NHS Digital Incident Reporting Tool housed in the Data Security and Protection Toolkit (DSPT).

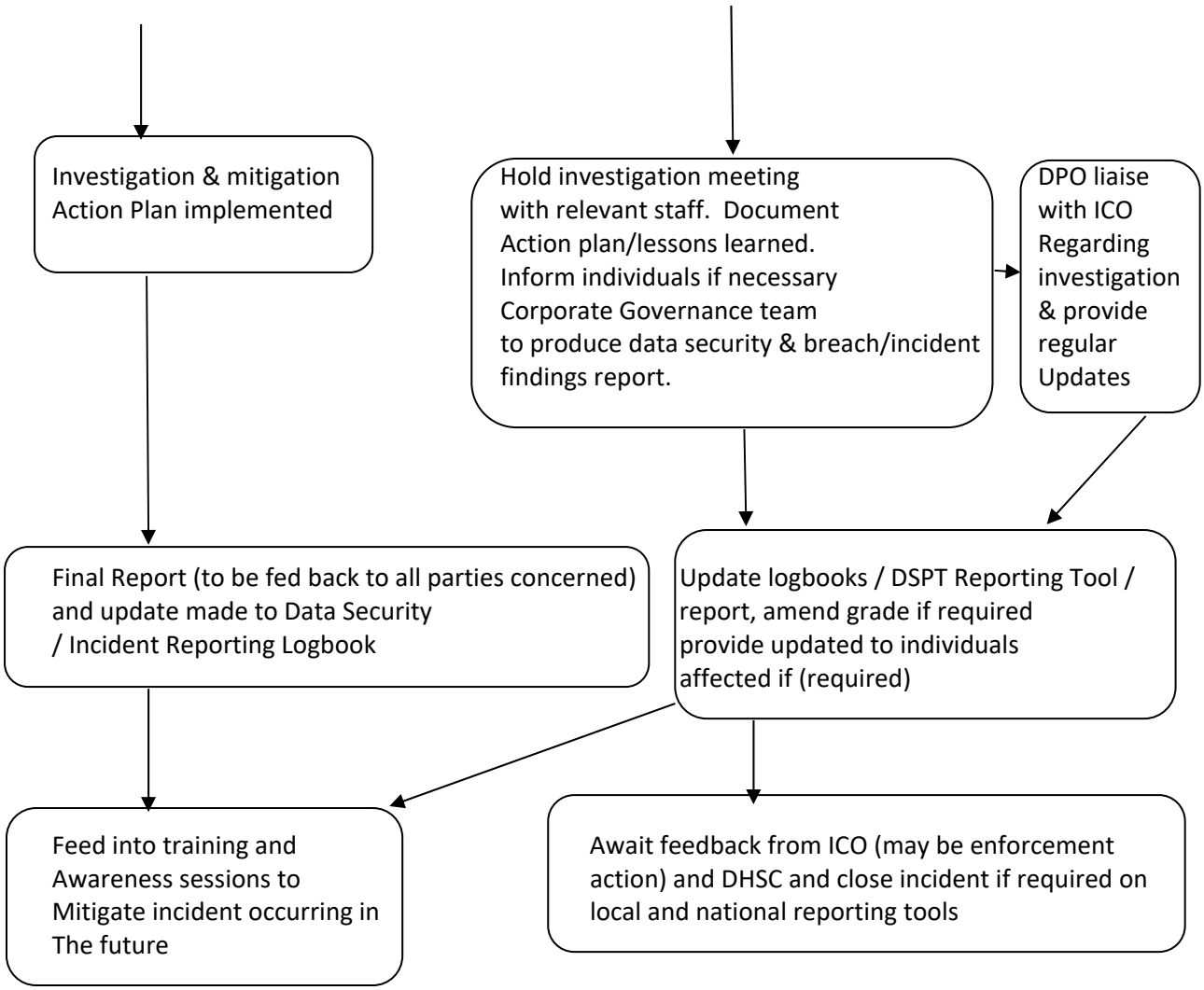
9. Time scale for reporting

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'.

10. Appendix A – Data Security Breach / Incident Reporting Flowchart




Investigation & mitigation Action Plan implemented
Hold investigation meeting with relevant staff. Document Action plan/lessons learned. Inform individuals if necessary Corporate Governance team to produce data security & breach/incident findings report.
DPO liaise with ICO Regarding investigation & provide regular Updates
Final Report (to be fed back to all parties concerned) and update made to Data Security / Incident Reporting Logbook
Update logbooks / DSPT Reporting Tool / report, amend grade if required provide updated to individuals affected if (required)
Feed into training and Awareness sessions to Mitigate incident occurring in The future
Await feedback from ICO (may be enforcement action) and DHSC and close incident if required on local and national reporting tools

11. 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 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 Information Governance Operational Group

Data Security breaches / incidents are reported routinely at the Information Governance Operational Group. Lessons learned are discussed and actioned when necessary to assist mitigation future similar incidents.

12. Lessons Learned

It is essential that action is taken to help to minimise the risk of data security breaches / incidents re-occurring in the future. Therefore, lessons learned from data security breaches will be fed back to staff. This may be communicated via email / staff briefings
And via communications.

Staff involved with a data security breach / incident will also be required to complete additional IG Training and / or require further support. The investigation team and / or IG Team will

determine this.

13. Training and Awareness

This procedure will be made available to all staff in reception and published on the CCG Website

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

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

- policy and procedure;
- line manager
- other communication methods (e.g. staff brief/team meetings).
- All staff are mandated to undertake Data Security Awareness training on an annual basis.

14. Monitoring and Review

Performance will be reviewed on an annual basis and used to inform the development of future procedural documents.

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
- Changes to organisational infrastructure

15. Appendix B

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.

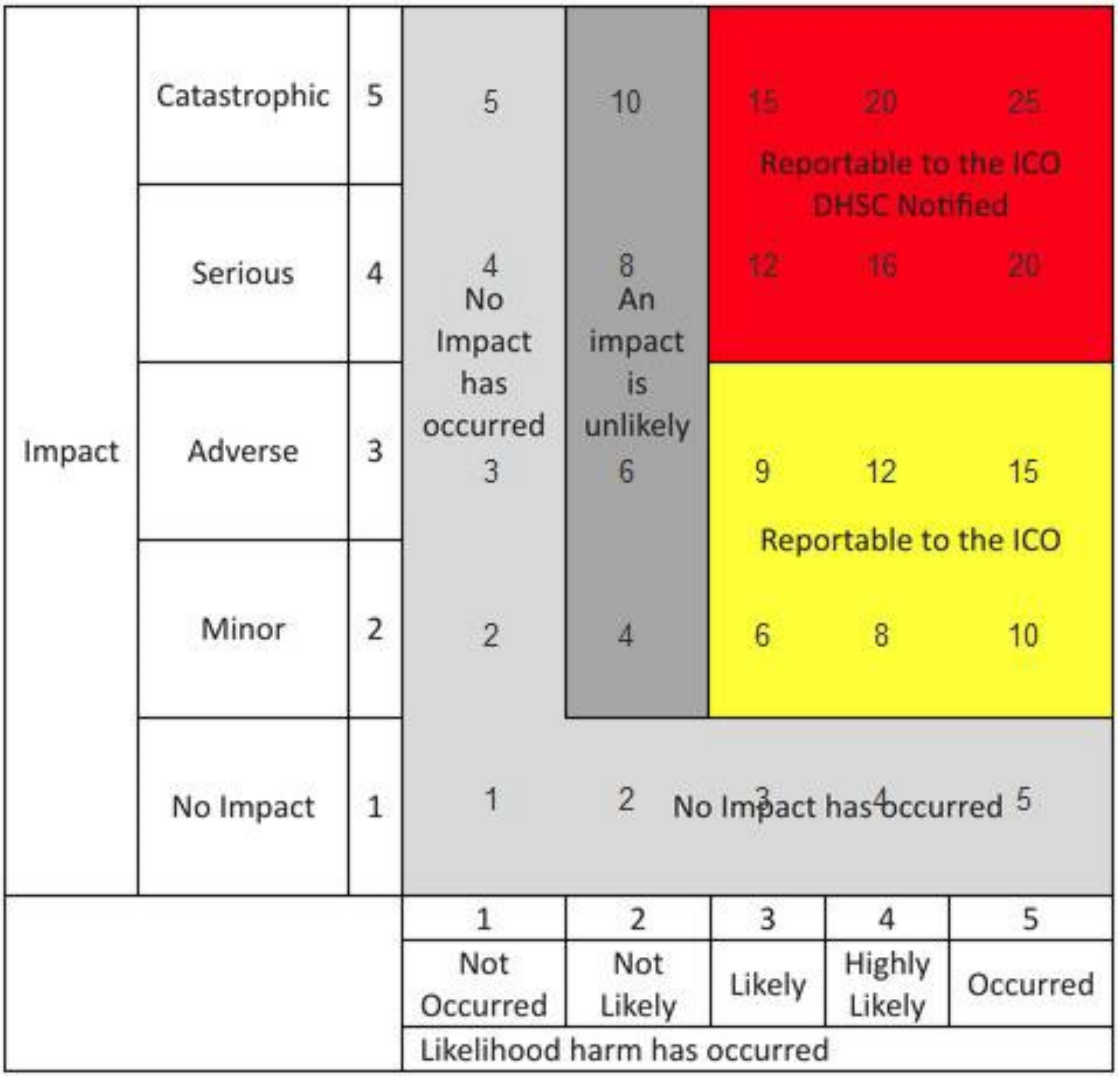
No	Effect	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach.
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred.	A minor adverse effect must be selected where there is no absolute 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 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.

16. Appendix C

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.



17. Appendix D - Summary

Reporting a Data Security Breach/Incident

A data security breach involves the loss of, or unauthorised access to, personal, confidential or business sensitive data. This includes both information in hard-copy and electronic information.

Examples of a breach can include:

- The loss or theft of data in any format (e.g. papers taken from car)
- Loss or theft or equipment used to store CCG Information (e.g. laptop, smartphone, USB stick)
- Inappropriate access controls allowing unauthorised access
- Compromised IT user account (e.g. hacking, shared password)
- Accidental or unauthorised disclosure of personal Information (e.g. email or letter to wrong recipient or incorrect system permissions)

- Break-in at a location holding sensitive information
- Computer systems or equipment compromise (e.g. virus)
- Corruption or unauthorised modification of vital records (e.g. alteration of master records)
- All information security incidents (including those involving paper records) must be reported promptly so the risk to individuals, Walsall CCG and others can be contained and prevented where possible

What is the difference between an Incident and a Breach?

- An information security incident is where there is the risk of a breach; by reporting these quickly, steps can be taken to investigate, secure the information and prevent the incident becoming a breach
- By reporting an incident we cannot only prevent a breach occurring, but can also learn where our risks are and identify controls to reduce the risk of them reoccurring
- An information security breach is where the incident has resulted in any loss of, or unauthorised access to data, normally involving personal or confidential information

Any information security breach that involves personal information is a breach of the Data Protection Act 2018. Walsall CCG needs to investigate, and when appropriate report these to the Information Commissioners Office who can issue enforcement action including fines.

You must report any perceived breaches as soon as possible (at least within 24 hours) **to Sara Saville or Serena Ellis** so they can be fully investigated. Ignoring them allows the information to go unchecked and the risk to individuals and the CCG to increase, therefore staff are more likely to receive a disciplinary for not reporting a security incident or breach.

What impact will the General Data Protection Regulation (GDPR) have on breaches?

Under the new law it is mandatory to report breaches to the ICO and we will need to ensure we have reported the breach within 72 hours of identifying the breach. We can get fined for data breaches, we can also get fined for not reporting a data breach.

How much are data breach fines?

The size of fine is relevant to the risk, if we quickly report, investigate and manage the data breach we can reduce the risks to individuals and this can reduce the amount the CCG is fined.