NHS
Greater Manchester Shared Services

# Data Security and Protection Breaches

# Incident Reporting Procedure

**Review Date: September 2020**

Greater Manchester Shared Services
Hosted by NHS Oldham CCG
on behalf of the Greater Manchester CCGs

## Document Control

| | |
|---|---|
| **Programme:** | Greater Manchester Shared Services |
| **Filename:** | I:GMSS/IG Policies & Procedures |
| **Author:** | IG Team |
| **Version:** | 0.1 |
| **Date Released:** | |
| **Purpose of this document:** | This document outlines GMSS Incident Reporting Process |

### Document Location

Copies of this document can be obtained from|:

| | |
|---|---|
| **Name:** | Corporate Services Office |
| **Address:** | Greater Manchester Shared Services<br>Ellen House<br>Waddington Street<br>Oldham<br>OL9 6EE |
| **Telephone:** | 0161 212 4186 |

### Revision History

| Revision date | Revision by | Summary of changes | Version |
|---|---|---|---|
| Sept 2018 | IG Team | New procedure | 0.1 |
| | | | |

### Approvals

| Name | Role | Date | Version |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

### Distribution

| Name | Role | Date | Version |
|---|---|---|---|
| Saved in policy folder | | | |
| Updated Policy Tracker | | | |
| GMSS Publication scheme | | | |
| Shared in the Bulletin | | | |

### DOCUMENT STATUS:

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of the document are not controlled.

## Contents

## 1. Introduction

Greater Manchester Shared Services (known hereafter as GMSS) 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).

This procedure describes the process for staff to follow regarding recording, reporting and reviewing of data security & protection breaches / incidents. This supports GMSS’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 (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 GMSS must keep a record of any personal data breaches, regardless of whether it is required to notify these to the ICO. The IG Team co-ordinate and maintain a Data Security Breaches / Incident Reporting Logbook.

GMSS 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 GMSS for the reporting and management of Data Security & Protection breaches / incidents.

This procedure applies to those members of staff directly employed by GMSS and for whom GMSS has legal responsibility.

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 GMSS.

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

## 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,
- 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:

- 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 know known as the European Data

Protection Board (EDPB) under the EU General Data Protection Regulation (GDPR) categorised data security breaches into 3 categories which were associated with confidentiality, integrity and / or availability.

Confidentiality
Integrity
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<br>(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 |
| 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 |

| | ICO Categorisation | Type of Breach<br>(Art 29 Working Party) |
|---|---|---|
| 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 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 & Protection incidents (DS&P).

### Data Protection Officer

To provide advice and guidance around the grading and categorisation of any DS&P 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, if this is likely to result in a high risk to the rights and freedoms of individuals.

### Senior Information Risk Owner (SIRO)

To review DS&P incidents and report issues to the 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 DS&P incidents, maintain an Incident / Data Security Breaches Reporting Logbook, make recommendations and act on lessons learnt.
- To liaise with GMSS Information Governance Lead, DPO, SIRO and IT Services / IT Security Manager as appropriate pertaining to data security incidents.

- To escalate incidents to GMSS Information Governance Lead in order to inform the Senior Information Risk Owner / Caldicott Guardian / DPO as appropriate.
- To grade the incident and report it where necessary on the Data Security & Protection Toolkit Incident Reporting Tool in conjunction with the DPO and log on the local IG Incident / Data Breaches Reporting Logbook.

### GMSS IT Services

To alert GMSS IT Security Manager and IG Team when a member of GMSS staff reports a potential or actual information security / IT / cyber security incident that is reportable as per the NHS Digital process via the IT Service Desk so this can 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 the ICO / NHS Digital.

## 5. Data Security Breaches / Incident Investigation Process

Staff must follow GMSS's process for incident reporting which includes any data security breaches / incidents. All data security breaches / incidents must be reported initially to GMSS IG Lead / DPO / IG Team AS SOON AS THIS INCIDENT IS KNOWN following GMSS's incident reporting processes. Please do not delay reporting of any incident even if you suspect it may not be an incident / breach. If it is identified as a data security breach / incident, it will be logged on GMSS Data Security Beaches / Incident Reporting Logbook. GMSS Lead / SIRO / CG / DPO and IG Team 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 GMSS 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 A 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 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).

### 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 GMSS 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 GMSS 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.

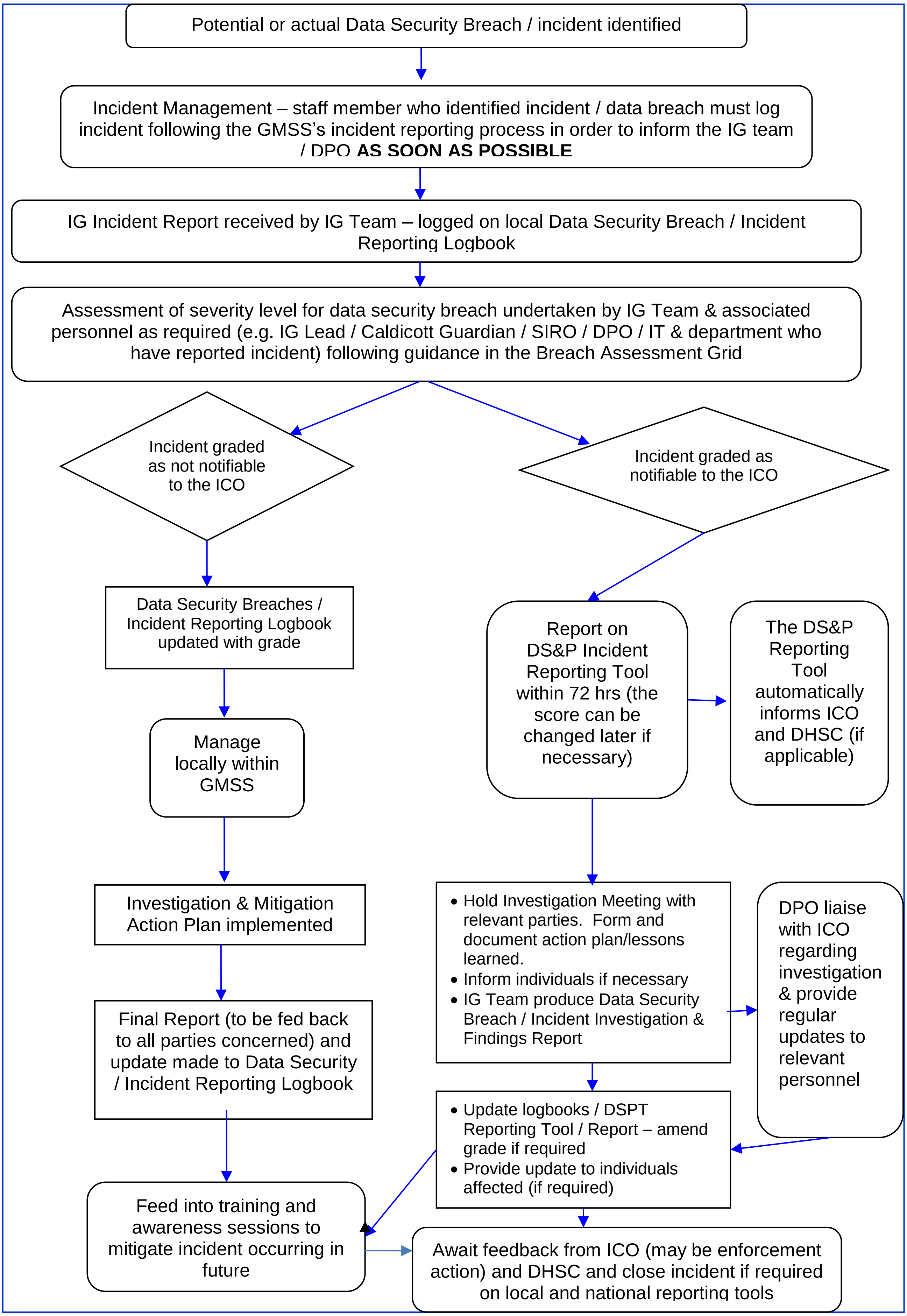
### Containment Actions which affect notification status

There may be circumstances where GMSS 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 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, GMSS could still possibly trust the recipient not to take any further action and return and co-operate with GMSS’s instructions
- Where GMSS 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 & protection incidents / personal data breaches for GMSS.

## Figure 1 – Data Security Breach / Incident Reporting Flowchart


Potential or actual Data Security Breach / incident identified
Incident Management – staff member who identified incident / data breach must log incident following the GMSS's incident reporting process in order to inform the IG team / DPO **AS SOON AS POSSIBLE**
IG Incident Report received by IG Team – logged on local Data Security Breach / Incident Reporting Logbook
Assessment of severity level for data security breach undertaken by IG Team & associated personnel as required (e.g. IG Lead / Caldicott Guardian / SIRO / DPO / IT & department who have reported incident) following guidance in the Breach Assessment Grid
Incident graded as not notifiable to the ICO
Incident graded as notifiable to the ICO
Data Security Breaches / Incident Reporting Logbook updated with grade
Manage locally within GMSS
Report on DS&P Incident Reporting Tool within 72 hrs (the score can be changed later if necessary)
The DS&P Reporting Tool automatically informs ICO and DHSC (if applicable)
Investigation & Mitigation Action Plan implemented
Hold Investigation Meeting with relevant parties. Form and document action plan/lessons learned.
Inform individuals if necessary
IG Team produce Data Security Breach / Incident Investigation & Findings Report
DPO liaise with ICO regarding investigation & provide regular updates to relevant personnel
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 update to individuals affected (if required)
Feed into training and awareness sessions to mitigate incident occurring in future
Await feedback from ICO (may be enforcement action) and DHSC and close incident if required on local and national reporting tools

## 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 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 IG Group

Data Security breaches / incidents are reported routinely at the Information Governance Group Meeting via the IG Key Statistics Report. Lessons learned are discussed and actioned when necessary to assist mitigation future similar incidents.

## 7. 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 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.

## 8. Training and Awareness

This procedure will be made available to all staff via GMSS bulletin and published on GMSS Website

All staff are responsible for adhering to the General Data Protection Regulations, Caldicott Principles, the NDG Data Security Standards, 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/strategy and procedure manuals;
- line manager;
- other communication methods (e.g. staff brief/team meetings, advisories).
- All staff are mandated to undertake Data Security Awareness training on an annual basis.

## 9. 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; and
- Changes to organisational infrastructure.

## Appendix A

## 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 |

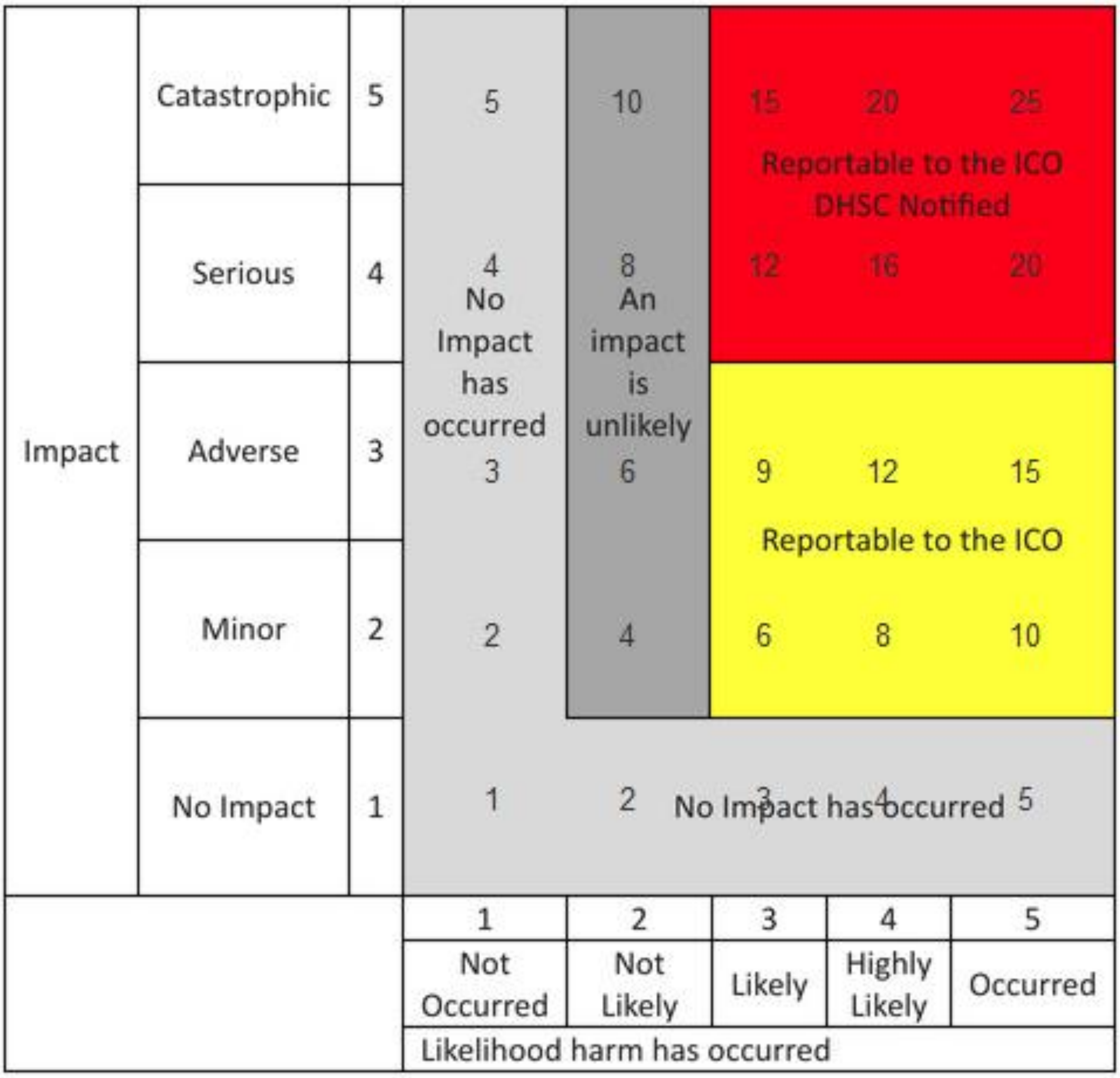
Both the adverse effect and likelihood values form part of the breach assessment grid.

## Appendix B

## 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.



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