Tarbock Medical Centre

|  |
| --- |
| **Data Security & Protection Breaches / Incident Reporting Policy and Procedure**  **Version No: [2.0]**  **Document Summary:**  To provide all staff with the information they need to follow the process when reporting Data Protection Incidents. |

|  |  |  |
| --- | --- | --- |
| **Document status** | Approved | |
| **Document type** | Policy | **local** |
| **Document number** | Document Control will provide document number if a new document | |
| **Approving body** | Information Governance Steering Group | |
| **Date approved** | 16/11/2021 | |
| **Date implemented** | 16/11/2021 | |
| **Review date** | **30/11/2024** | |
|  | **Reviewed June 2025, no changes made** | |
| **Accountable Director** | Choose an item. | |
| **Policy Author** | Head of Risk Assurance & DPO | |
| **Target audience** | All staff | |

**The intranet version of this document is the only version that is maintained. Any printed copies should therefore be viewed as “uncontrolled”, as they may not contain the latest updates and amendments.**

# Document Control

**[Author to complete all sections apart from Section 4 & 5]**

|  |  |  |  |
| --- | --- | --- | --- |
| **Section 1 – Document Information** | | | |
| **Title** | **Data Security & Protection Breaches / Incident Reporting Policy and Procedure** | | |
| **Directorate** | | Informatics | |
| **Brief Description of amendments** | | | |
| Click here to enter text.  ***Please state if a document has been superseded.*** | | | |
| **Does the document follow the Practice agreed format?** | | | Yes |
| **Are all mandatory headings complete?** | | | Yes |
| **Does the document outline clearly the monitoring compliance and performance management?** | | | Yes |
| **Equality Analysis completed?** | | | Yes |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Section 2 – Consultation Information** | | | | |
| **Consultation Completed** | |  | | |
| **Consultation start date** | 07/07/2020 | | **Consultation end date** | 28/07/2020 |

|  |  |  |
| --- | --- | --- |
| **Section 3 – Version Control** | | |
| **Version** | **Date Approved** | **Brief Summary of Changes** |
|  | Click here to enter a date. |  |
|  | Click here to enter a date. |  |
|  | Click here to enter a date. |  |
|  | Click here to enter a date. |  |
|  | Click here to enter a date. |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Section 4 – Approval** *– To be completed by Document Control* | | | | |
| **Document Approved** | |  | | |
| **Assurance provided by Author & Chair** | |  | | |
| **Date approved** | Click here to enter a date. | | **Review date** | Click here to enter a date. |

|  |  |  |
| --- | --- | --- |
| **Section 5 – Withdrawal** *– To be completed by Document Control* | | |
| **Reason for withdrawal** | |  |
| **Assurance provided by Author & Chair** | |  |
| **Date Withdrawn:** | Click here to enter a date. | |

Contents

[Document Control 2](#_Toc69818756)

[1. Scope 4](#_Toc69818757)

[2. Introduction 4](#_Toc69818758)

[3. Purpose 5](#_Toc69818759)

[4. Definitions 6](#_Toc69818760)

[5. Duties, Accountabilities and Responsibilities 9](#_Toc69818761)

[6. Investigations 11](#_Toc69818762)

[7. Data Breach / Incident Investigation Process 11](#_Toc69818763)

[8. Reporting 18](#_Toc69818764)

[9. Closure and Lessons Learned 18](#_Toc69818765)

[10. Training and Awareness 19](#_Toc69818766)

[11. Monitoring Compliance 19](#_Toc69818767)

[12. References 20](#_Toc69818768)

[13. Related Practice Documents 20](#_Toc69818769)

[14. Equality Analysis Form 21](#_Toc69818770)

[Appendix 1 – Current ICO Breach Categorisations 22](#_Toc69818771)

[Appendix 2 – Data Security and Protection Breach / Incident Investigation Report Form 24](#_Toc69818772)

# Scope

This document is to inform **ALL** staff of the process for reporting personal data breaches and the process that the Practice’s Information Governance (IG) Team and all employees must follow so there is no ambiguity. This Policy and Procedure is Practice wide and is therefore applicable to all Departments and functions at The Practice. This is to protect the individual’s rights and freedoms of our patients and staff and to protect the Practice as a Data Controller.

# Introduction

Tarbock Medical Centre (henceforth referred to as ‘the Practice’) is committed to a programme of effective risk and incident management and has a responsibility to ensure personal data breaches and / or information governance incidents are reported and managed efficiently and effectively.

The UK General Data Protection Regulation (UK GDPR) brought in in May 2018 requires that where personal data breaches affect the ‘rights and freedoms of an individual,’ Article 33 (of the UK GDPR) imposes a duty to report these types of personal data breach to NHS Digital and to the Information Commissioner’s Office (ICO), the supervisory authority, within 72 hours of becoming aware of it.

The Practice will ensure robust breach detection, investigation, and internal reporting procedures are in place which comply with legislative timescales for reporting through the implementation of this policy and procedure. 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 Practices overall incident reporting process which is an integral part of personal, clinical and corporate governance.

For the purposes of this policy and procedure the breach / incident will only be reviewed and investigated if the data concerns ‘personal data’ and may affect the rights and freedoms of an individual / data subject it relates to. The UK GDPR is the legal framework that provides guidelines to data controllers to ensure they protect individual’s personal data when it is being processed.

The information contained within this procedure is taken from the “Guide to the Notification of Data Security and Protection Incidents” produced by NHS Digital. 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](http://www.dsptoolkit.nhs.uk/Help/29)

The Practice will use the NHS Digital Data Security and Protection Incident Reporting tool (accessed through the Data Security and Protection Toolkit) for the purposes of notifying breaches on one form, which will be shared across several regulatory agencies. These include personal data breaches of the UK GDPR to the ICO and cyber security incidents to NHS Digital. Security of Network Information Systems Regulations or NIS incidents are also reportable, and these are forwarded to the Department of Health and Social Care (DHSC) where appropriate.

The Practice will comply with the National Data Guardian Data Security Standard six to provide evidence of their compliance with personal data breaches in the Data Security and Protection Toolkit:

*“Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.”*

*“All staff are trained in how to report an incident, and appreciation is expressed when incidents are reported. Sitting on an incident, rather than reporting it promptly, faces harsh sanctions. The Board understands that it is ultimately accountable for the impact of security incidents, and bears the responsibility for making staff aware of their responsibilities to report upwards. Basic safeguards are in place to prevent users from unsafe internet use. Anti-virus, anti-spam filters and basic firewall protections are deployed to protect users from basic internet-borne threats.”*

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 Practice must keep a record of any personal data breaches, regardless of whether it is required to notify these to the ICO and / or NHS Digital. The Practices IG Team will maintain a local data security breaches / incident reporting logbook and also use an incident management system to fully record the particulars of all incidents, investigations and remedial actions.

# Purpose

The Practice is committed to a programme of effective risk identification and information risk management through the consistent reporting, monitoring and review of incidents that result, or have the potential to result in confidentiality breach, damage or other loss, also known as data breaches.

The Practice also recognise the importance of ‘near-miss’ breaches along with actual breaches.

The benefits of all types of breaches include:

* Increasing awareness
* Addressing resource issues
* Identifying gaps in training
* Identifying trends across the Practice
* Pre-empting similar breaches / complaints
* Demonstrating the Practice’s response

This document sets out the directions across the Practice for the reporting and management of personal data breaches / incidents, including Serious Incidents Requiring Investigations (SIRIs).

It is the responsibility of all staff to ensure that information remains secure where this is required and therefore, it is important that when incidents occur, damage from them is minimised and lessons are learnt from them.

This procedure applies to all staff who work for or on behalf of the Practice and for whom the Practice 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 the Practice.

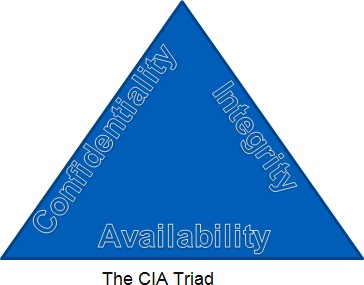
Further, this procedure applies to all third parties and others authorised to undertake work / process data on behalf of the Practice.

# Definitions

|  |  |
| --- | --- |
| Definition | **Meaning** |
| Adverse Effect | Any untoward occurrence which can be unfavourable and an unintended outcome associated with an incident. |
| Cyber Incident | There are many possible definitions of what a cyber incident is. For the purposes of reporting, a cyber incident is defined as anything that could (or has) compromised information assets within cyberspace. ‘Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services.’ It is expected that the type of incidents reported would be of a serious enough nature to require investigation by the organisation. These types of incidents could include, denial of service attacks, phishing emails, social media disclosures, web site defacement, malicious internal damage, spoof website, cyber bullying. |
| Data Controller | A data controller determines the purposes and means of processing personal data. |
| Data Processor | A processor is responsible for processing personal data on behalf of a controller. |
| Destruction | This is where the data no longer exists, or no longer exists in a form that is of any use to the controller. |
| Loss | The data may still exist, but the controller has lost control or access to it, or no longer has it in its possession. |
| Near Miss | A near miss is an incident that had the potential to cause harm but was prevented. These include clinical and non-clinical incidents that did not lead to harm or injury, disclosure or misuse of confidential data but had the potential to do so. |
| 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:   * 1. an identifier such as a name, an identification number, location data or an online identifier, or   2. 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. The UK GDPR also introduces geographical data and biometric data to be classified as personal data. |
| Personal Data Breach | As per Article 4(12) of the UK 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. |
| Processing | This means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |
| Serious Incident Requiring Investigation (SIRI) | Serious Incident Requiring Investigations (SIRIs) are incidents which involve actual or potential failure to meet the requirements of data protection legislation and/or the Common Law Duty of Confidentiality. This includes unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people’s privacy. This definition applies irrespective of the media involved and includes both electronic media and paper records. When lost data is protected e.g. by appropriate encryption, so that individuals data cannot be accessed, then there is no data breach (though there may be clinical safety implications that require the incident to be reported via a different route). |
| Special Category Data | Special category data is personal data relating to:  (a) racial or ethnic origin of the data subject  (b) political opinions  (c) religious beliefs or other beliefs of a similar nature  (d) member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998  (e) genetic data  (f) biometric data for the purpose of uniquely identifying a natural person  (g) physical or mental health or condition  (h) sexual life or sexual orientation  For data security breach reporting purposes, special category 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 |
| Unauthorised Processing | Unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the UK GDPR. |

Breach Types

The Article 29 working party, was 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 (UK GDPR) from 25th May 2018 categorised data security breaches into 3 categories which were associated with confidentiality, integrity and / or availability. These are still applicable under the UK GDPR.



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

Confidentiality Breach Example

Infection by ransomware (malicious software which encrypts the controller’s data until a ransom is paid) could lead to a temporary loss of availability if the data can be restored from backup. However, a network intrusion still occurred, and notification could be required if the incident is qualified as confidentiality breach (i.e. personal data is accessed by the attacker) and this presents a risk to the rights and freedoms of individuals. If the attacker has not accessed personal data, the breach would still represent an availability breach and require notification if the potential for a serious impact on the rights and freedoms of the individual.

Availability Breach Example

In the context of a hospital, if critical medical data about patients are unavailable, even temporarily, this could present a risk to individuals’ rights and freedoms; for example, operations may be cancelled. This is to be classified as an availability breach.

Integrity Breach Example

Where a health or social care record has an entry in the wrong record (misfiling) and has the potential of significant consequences it will be considered an integrity breach. For example, a ‘do not resuscitate’ notice on the wrong patient record may have the significant consequence of death whilst an entry recording the patient blood pressure may not have the same significant result.

# Duties, Accountabilities and Responsibilities

Senior Partners

The Practice Senior Partners has ultimate responsibility for the implementation of the provisions of this procedure. As the ‘Accountable Officers’ 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 required as per the UK GDPR. The DPO’s role is to inform and advise the Practice and its staff about their obligations to comply with the UK GDPR and other current data protection laws. They are required to monitor compliance with the UK 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 ensure where a breach results in a risk to the rights and freedoms of data subjects the ICO is informed no later than 72 hours after the Practice becomes aware of the incident.

Caldicott Guardian

The Caldicott Guardian is the person within the Practice that has overall responsibility for protecting the confidentiality of personal data and special category data, and for ensuring it is shared appropriately and in a secure manner. Where a data breach relates to patient data they will be asked to review and provide feedback. This may involve decision making about informing patients regarding an incident or not if this would deem to cause them harm / distress.

Practice Manager

The Practice Manager is allocated lead responsibility for the Practice’s Information Governance Framework. The Practice Manager must provide the “Accountable Officer” with assurance that information risk is being managed appropriately and effectively across the Practice and for any services contracted by the organisations. Where data breaches concern information risks, they are asked to review and report to the Caldicott Guardian and Senior Partners. They must be provided with assurances that the incident has been reported to the ICO if required.

Information Asset Owners (IAOs)

The Information Asset Owners (IAOs) support the Practice Manager and will support the IG team when data breaches concerning their department arise. They will:

* be identified, provided with training and support and will carry out risk assessments on the information assets, to protect against unauthorised access or disclosure, within their area;
* ensure the integrity of the information within their area and restrict the use to only authorised users who require the access;
* be responsible for the Information Asset assigned to them;
* help establish an action plan / lesson learned from data breaches that arise in their area.

Information Governance Team

The Information Governance Team will support the organisation in investigating incidents, offer advice and ensure the organisation complies with legislation, policies and protocols, and will:

* co-ordinate and investigate reported data and security protection incidents, maintain the Practice Data and Security breaches in Elaine and, make recommendations and act on lessons learnt.
* liaise with the, DPO, Senior Partner, Caldicott Guardian and IT Services as appropriate pertaining to data security incidents.
* escalate incidents to the DPO.
* grade the incident and report it where necessary on the Data Security and Protection Toolkit Incident Reporting Tool in conjunction with the DPO and log on the local Practice IG Incident / Data Breaches Reporting Logbook and the incident management system.

IT Leads

* To work with IT Services and in particular the Information Security team to investigate incidents where IT and IT Security input is required, make recommendations and act on lessons learnt;
* To inform the DPO, Practice Manager, Senior Partner, Caldicott Guardian as appropriate.

Information Security Team

To alert the Practice IT Leads, DPO and IG team when a member of 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 will be investigated, reported and graded accordingly following 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.

Practice 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 Practice and this extends after they have left the Practice. All members of staff must read and sign the Confidentiality Code of Conduct.

Practice’s Information Governance (IG) Steering Group

The Practice Information Governance Steering Group is responsible for overseeing the Practice’s IG framework and agenda ensuring its compliance with Data Protection. Personal data breaches are reported to this Group demonstrating that the reporting incident process has been followed and provides assurance that any actions arising are being monitored and carried out, these include near miss breaches / incidents.

# Investigations

The purpose of a breach / incident investigation is to:

* carry out a root cause analysis in order to establish what actually happened and what actions and recommendations are needed to be taken to prevent reoccurrence
* identify whether any areas of improvement of the Practice’s IG policies or procedures
* determine whether a human error has occurred, but not to allocate blame
* decide whether to notify the data subject. This decision will be made by Data Protection Officer and depending on the type of breach may involve the Practice Senior Partners and the Caldicott Guardian. In some cases the investigation may identify whether any disciplinary processes may need to be invoked.

# Data Breach / Incident Investigation Process

Reporting and Recording the incident

All data breaches / incidents must be reported to the IG Team AS SOON AS THIS INCIDENT IS KNOWN following the Practice’s incident reporting processes (detailed below in the flowchart). Staff should not delay the reporting of any incident even if unsure whether it may not be a breach / incident. The IG Team will assess whether it is classed as a data breach. If it is identified as a data breach / incident, it will be immediately logged on the Practice’s Data Breaches / Incident Reporting Logbook. and the IG Team will assess the data breach accordingly using the grading system detailed below. The IG Team will seek guidance from the DPO if the data breach is scored high and may need to be reported to the ICO. If this concerns patient data the IG Team will also seek the advice from the Caldicott Guardian. Before any data breaches are reported to the ICO the DPO will seek approval from the Practice Senior Partners and Practice Manager.

Staff should report data breach / incidents via the ‘Practice Significant Event Register’ incident reporting tool by entering their Practice username / password (same details used to access Practice computers).

If a member of staff has no access to the intranet, details should be reported to [<insert](mailto:ithelpdesk@sthk.nhs.uk) practice IT contact details>

The immediate response to a breach / 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 Protection /Security/ IG incident the IG Team will be notified from the system.

Grading the Data Breach / Incident

Grading of the severity of a breach / incident will be made using the grading system detailed in the NHS Digital Data Security and Protection Incident Reporting Guidance. This grading system identifies which incidents are notifiable to external organisations such as the ICO and NHS Digital.

Within the grading system the factors for assessing the severity level of incidents are impact and likelihood these are detailed below.

Where the breach relates to a vulnerable group in society, as defined below, the minimum score will be a 2 in either significance or likelihood unless the incident has been contained.

Where vulnerable is a ‘Child known to safeguarding or with mental health conditions. Adult with capacity issues or known to adult safeguarding’

Likelihood: 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. |

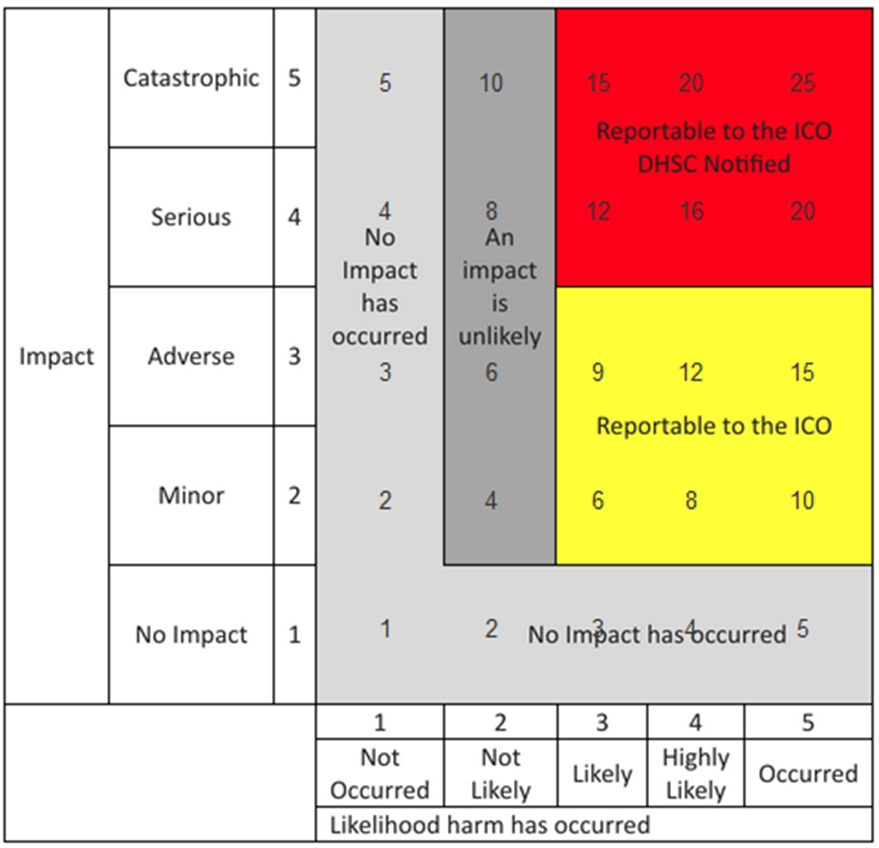
If the likelihood that an adverse effect has occurred is low and the breach is not reportable to the ICO, no further details will be required.

Impact: 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.

Once Impact and Likelihood have been assessed the incident grading is found using the matrix below:



Where the breach is assessed that it is (at least) likely that some harm has occurred and that the impact is (at least) minor, the incident is reportable and full details will be automatically emailed to the ICO and the NHS Digital Data Security Centre.

Sensitivity Factors

Sensitivity factors have been incorporated into the grading scores and where a non-notifiable personal data breach involves one of the following categories of data, the breach assessment must start at ‘minor impact’ and ‘harm not likely’ scoring it at 2 x 2 = 4. It will only be reportable to the ICO where further assessment increases along the likelihood of harm axis:

* Vulnerable children
* Vulnerable adults
* Criminal convictions / prisoner information including the alleged commission of offences by the data subject or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing
* 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
* Special Categories data (this includes health data)

Containment Actions which affect notification status

There may be circumstances where the Practice 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 (The Practice) 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 Practice could still possibly Practice the recipient not to take any further action and return and co- operate with the Practice’s instructions.
* Where the Practice can null the effect of any personal data breach.

Assessing risk to the rights and freedoms of a data subject (likelihood)

The UK GDPR gives interpretation as to what might constitute a high risk to the rights and freedoms of an individual. This may be any 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

A tabular conversion table at in Appendix 2 lists how previous data breach reporting maps to the ICO categorisations. A full list of rights and freedoms is given at the following link and the above are a summary of the main results of a breach on those rights.

<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>

External Notification of the Breach

Under Article 33 of the UK GDPR the Practice is required to notify the ICO of these breaches. . 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.

Where a breach has involved an external organisation, the Practice will ensure that they are notified of the outcome, particularly if the incident is reported to the ICO.

Time scale for reporting

Article 33 of the UK GDPR requires reporting of a breach within 72 hours. This is from when the Practice becomes aware of the breach and may not be necessarily when it occurred. However, it is important that all staff report any 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’.

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

Informing the data subject / individual

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 Practice decides not 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.

Data Security & Protection Breach / Incident Investigation Report Form

Where serious near miss breaches or reportable breaches occur the IG Team along with the relevant team / party will complete a ‘Data Security & Protection Breach / Incident Investigation Report Form’ (please refer to Appendix 2). This will ensure that the grading of the incident is followed in line with the process highlighted in this section.

This form will detail the breach, who should be informed, the grading, findings, lesson learned and an action plan with dates. Staff will be required to carry out their actions and feedback, this will provide assurance to the Practice (and others) that the incident has been taken seriously and plans are in place to reduce similar breaches. The form will be distributed to the appropriate members of staff and shared with relevant organisations and the data subject / individual if relevant.

Figure 1 – Data Security Breach / Incident Reporting Flowchart

Potential or actual Personal Data Breach / incident identified

Incident Management – staff member who identified data breach must log incident following the Practice incident reporting process (via the Practice Significant Event Register ) in order to inform the IG team

**AS SOON AS POSSIBLE**

Data breach /received by IG Team – logged on local Data Breach / Incident Reporting Logbook

Assessment of severity level for data security breach undertaken by IG Team & associated personnel as required (e.g. Practice IG Lead / Caldicott Guardian / Senior Partners / DPO / IT & department who have reported incident) following guidance in the Breach Assessment Grid

Incident graded as NOT reportable to the ICO

Incident graded as **reportable** to the ICO

Update Significant Event Register or Data Breaches / Incident Reporting Logbook updated with grade

Manage investigation locally within the Practice

Report on   
DSPT within 72 hrs (the score can be changed later if necessary)

Investigation & Mitigation Action Plan implemented

Final findings / report (to be fed back to all parties concerned including IGSG) and update made to Data Security / Incident Reporting Logbook

Await feedback from ICO (may be enforcement action) and DHSC and close incident if required on local and national reporting tools

Feed into training and awareness sessions to mitigate incident occurring in future

* 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

Update outcome of investigation to:

* ICO
* Senior Partners
* Caldicott Guardian
* Significant event register
* Affected individuals

DPO liaise with ICO regarding investigation & provide regular updates to relevant personnel

The DSPT automatically informs ICO and DHSC (if applicable / score warrants it)

8. Reporting

Information Governance Steering Group

All personal data breaches will be reported to the Practices Information Governance Steering Group whether reportable or not. Incidents that score highly or are classed as serious near misses will be supported by a completed Data Security & Protection Breach / Incident Investigation Report Form to demonstrate that the breach was investigated, the grade and an action plan. Where near miss breaches occur actions / outcomes are noted on the data security breaches / incident reporting logbook which is presented at each meeting. The Group are able to identify the trends even in minor incidents. The Practices Information Governance Steering Group is Chaired by the Caldicott Guardian and attended by the Practice Manager, who will report any serious breaches to the Board

The Practice’s Executive Team

The Senior Partner is a member of the Practice’s Executive Team and will notify this group of any high risk / near miss incidents with information and assurance supplied by the IG team.

Reporting in the Annual Governance Statement / Statement of Internal Control

Reportable breaches 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 2 - Summary of Data and Protection 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 Data Security and Protection Toolkit 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.

# Closure and Lessons Learned

It is essential that action is taken to help to minimise the risk of data breaches re-occurring in the future. Therefore, all breaches 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 breach should consider with their line manager if additional training and support is needed, although this is likely to be identified in the action plan from the investigation. Line managers should contact the IG Team for further assistance.

# 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 Practice and this extends after they have left the employ of the Practice.

All staff are responsible for adhering to the General Data Protection Regulation, [Caldicott Principles](http://confidential.oxfordradcliffe.net/caldicott/caldicott/report/principles), the National Data Guardian Security Standards, the [Data](http://confidential.oxfordradcliffe.net/DPA) [Protection Act](http://confidential.oxfordradcliffe.net/DPA) 2018, 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 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 using the e-Learning module, when possible. There will be face to face sessions available via Teams with workbooks and test questions available from the intranet. The Training Needs Analysis will identify any staff groups that will require additional training.

In any event, ALL Staff must complete a test to comply with the 3rd National Data Guardian standard:

*“Data Security Standard 3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.”*

# Monitoring Compliance

Key Performance Indicators (KPIs) of the Policy

|  |  |
| --- | --- |
| **No** | **Key Performance Indicators (KPIs) Expected Outcomes** |
| 1 | Any changes in legislation in connection with data protection law |
| 2 | Data Security & Protection Toolkit (DSPT) |
| 3 | MIAA Audits |

Performance Management of the Policy

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Minimum Requirement to be Monitored** | **Lead(s)** | **Tool** | **Frequency** | **Reporting Arrangements** | **Lead(s) for acting on Recommendations** |
| Procedure | Head of Risk Assurance & DPO | DSPT | 3 yearly | IGSG | IGSG/ IG Team |

# References

|  |  |
| --- | --- |
| **No** | **Reference** |
| 1 | https://[www.dsptoolkit.nhs.uk/Help/29](http://www.dsptoolkit.nhs.uk/Help/29) |

# Related Practice Documents

A number of other policies should be read in conjunction with this policy and procedure document:

|  |  |
| --- | --- |
| **No** | **Related Document** |
| 1 | Information Governance Policy |
| 2 | Confidentiality Code of Conduct |
| 3 | Data Protection Policy |
| 4 | Information Governance Policy |

# Equality Analysis Form

The screening assessment must be carried out on all policies, procedures, organisational changes, service changes, cost improvement programmes and transformation projects at the earliest stage in the planning process to ascertain whether a full equality analysis is required. This assessment must be attached to all procedural documents prior to their submission to the appropriate approving body. A separate copy of the assessment must be forwarded to the Patient Inclusion and Experience Lead for monitoring purposes. <insert practice email>. If this screening assessment indicates that discrimination could potentially be introduced then seek advice from the Patient Inclusion and Experience Lead. A full equality analysis must be considered on any cost improvement schemes, organisational changes or service changes which could have an impact on patients or staff.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Equality Analysis** | | | | | | | | |
| **Title of Document/proposal /service/cost improvement plan etc:** | | | Data Security & Protection Breaches / Incident Reporting Policy and Procedure | | | | | |
| **Date of Assessment** | | 07/07/202 | | | **Name of Person completing assessment /job title:** | | | Camilla Bhondoo |
| **Lead Executive Director** | | Director of Informatics | | | Head of Risk Assurance & DPO |
| **Does the proposal, service or document affect one group more or less favourably than other group(s) on the basis of their:** | | | | **Yes / No** | | | **Justification/evidence and data source** | |
| **1** | Age | | | No | | | No applies to ALL Staff | |
| **2** | Disability (including learning disability, physical, sensory or mental impairment) | | | No | | | No applies to ALL Staff | |
| **3** | Gender reassignment | | | No | | | No applies to ALL Staff | |
| **4** | Marriage or civil partnership | | | No | | | No applies to ALL Staff | |
| **5** | Pregnancy or maternity | | | No | | | No applies to ALL Staff | |
| **6** | Race | | | No | | | No applies to ALL Staff | |
| **7** | Religion or belief | | | No | | | No applies to ALL Staff | |
| **8** | Sex | | | No | | | No applies to ALL Staff | |
| **9** | Sexual Orientation | | | No | | | No applies to ALL Staff | |
| **Human Rights – are there any issues which might affect a person’s human rights?** | | | | **Yes / No** | | | **Justification/evidence and data source** | |
| **1** | Right to life | | | No | | | Ensures staff comply with the law | |
| **2** | Right to freedom from degrading or humiliating treatment | | | No | | | Ensures staff comply with the law | |
| **3** | Right to privacy or family life | | | No | | | Ensures staff comply with the law | |
| **4** | Any other of the human rights? | | | No | | | Ensures staff comply with the law | |
| **Lead of Service Review & Approval** | | | | | | | | |
| **Service Manager completing review & approval**  **Job Title:** | | | | | | Click here to enter text. | | |
| Click here to enter text. | | |

# 

## Appendix 1 – Current ICO Breach Categorisations

The table below incorporates the Article 29 working party categorisation of Confidentiality, Integrity and Availability breaches against the historic SIRI and cyber SIRI classifications. Additionally, the last column has the current ICO categorisations for illustration in a like for like comparison of old to new.

The Article 29 working party ‘Breach Notification Guidance’ provides detailed guidelines on Personal data breach notification under Regulation 2016/679 to supplementary the GDPR guidance.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type of breach Art 29 WP** | **Sub type Art 29 WP** | **SIRI tool** | **Cyber SIRI tool** | **ICO Categorisation inc new cyber breach types** |
| Confidentiality | Unauthorised or accidental disclosure | B Disclosed in Error | Phishing emails | Data sent by email to incorrect recipient |
|  | H Uploaded to website in error | Social Media Platforms | Data posted or faxed to incorrect recipient |
|  | J Unauthorised Access/Disclosure | Spoof website | Failure to redact data |
|  |  | Cyber bullying | Information uploaded to webpage |
|  |  |  | Verbal disclosure |
|  |  |  | Failure to use bcc when sending email |
|  |  |  | Data sent by email to incorrect recipient |
|  |  |  | Cyber security misconfiguration (e.g. inadvertent publishing of data on website; default passwords) |
|  |  |  | Cyber incident (phishing) |
| Unauthorised or accidental access | I Technical security failing (including | Hacking | Insecure webpage (including hacking) |
|  | J Unauthorised Access/Disclosure |  | Cyber incident (key logging software) |
| Availability | Unauthorised or accidental loss | A) Corruption or inability to recover electronic data | Denial of Service (DOS) | Loss or theft of paperwork |
|  | C Lost In Transit |  | Loss or theft of unencrypted device |
|  | D Lost or stolen hardware |  | Loss or theft of only copy of encrypted data |
|  | E Lost or stolen paperwork |  | Data left in insecure location |
|  |  |  | Cyber incident (other – DDOS etc.) |
|  |  |  | Cyber incident (exfiltration) |
|  |  |  | Cryptographic flaws (e.g. failure to use HTTPS; weak encryption) |
| Unauthorised or accidental destruction | F Non-secure Disposal – hardware | Malicious internal damage | Insecure disposal of paperwork |
|  | G Non-secure Disposal – paperwork |  | Insecure disposal of hardware |
| Integrity | Unauthorised or accidental alteration | K Other | Web site defacement | Other principle 7 failure |
|  |  |  | Cyber incident – unknown (e.g. data published on Pastebin but no information on how compromise occurred) |

## Appendix 2 – Data Security and Protection Breach / Incident Investigation Report Form

**Data Security & Protection Breach / Incident Investigation Report Form**

|  |  |
| --- | --- |
| Local ID Reference: |  |
| Date: |  |

**Distribution List**

|  |  |  |
| --- | --- | --- |
| Name | Title | Organisation |
|  |  |  |
|  |  |  |

**Tracking Reference**

|  |  |
| --- | --- |
| Practice IG Incident Reference No : |  |
| STEIS Reference No: |  |
| ICO Reference No: |  |

**Amendment History**

|  |  |  |
| --- | --- | --- |
| **VERSION** | **DATE** | **AMENDMENT HISTORY** |
|  |  |  |
|  |  |  |

**Incident Roles / Contacts**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Title & Organisation** | **Role** | **Contact Details** |
|  |  |  |  |
|  |  |  |  |

**Contents**

[1. Data Security / Incident Breach Details 26](#_Toc524079489)

[2. Grading & RAG Rating 26](#_Toc524079490)

[3. Investigation Findings 28](#_Toc524079491)

[4. Outcomes 28](#_Toc524079492)

[5. Lessons Learned / Action Plan 29](#_Toc524079493)

**Data Security Incident Investigation Report**

1. Data Security / Incident Breach Details

| **Item** | **Details** |
| --- | --- |
| Local Data Breach / Incident ID Reference: |  |
| Date reported: |  |
| Name, Title, Dpt or person incident reported by: |  |
| Name of Team where incident / occurred: |  |
| Type of Record |  |
| ICO categorisation of data breach / incident |  |
| Description of the nature of the breach: |  |
| Description of the likely consequences of the personal data breach: |  |
| Description of the immediate measures taken: |  |
| Is the incident still on-going? |  |
| Does this incident relate to a vulnerable group in society? |  |

1. Grading & RAG Rating

Data Security breaches / incidents are graded according to the significance of the breach and the likelihood of those serious consequences occurring. The criteria is outlined in the “Guide to the Notification of Data Security and Protection Incidents.” This also informs when an incident is reportable to the ICO.

The classification of this data breach and grading is detailed in the table below:

|  |  |
| --- | --- |
| **Incident Grading and classification details** | **Grade / Classification** |
| **Categorisation of Incident** |  |
| **ICO categorisation of incident** |  |
| **Grading and RAG Rating** | Please score the incident using the 5x5 matrix as per below and detailed in the NHS Digital “Guide to the Notification of DS & Protection Incidents”. Please state the likelihood, impact and overall grade and RAG rating below.  Breach Assessment Grid   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | **Impact** | **5** | **5** | **10** | **15** | **20** | **25** | | **4** | **4** | **8** | **12** | **16** | **20** | | **3** | **3** | **6** | **9** | **12** | **15** | | **2** | **2** | **4** | **6** | **8** | **10** | | **1** | **1** | **2** | **3** | **4** | **5** | | **x** | **1** | **2** | **3** | **4** | **5** | |  |  | **Likelihood** | | | | |   Key   |  |  | | --- | --- | |  | Reportable to the ICO and HHSC | |  | Reportable to the ICO | |  | An impact is unlikely - manage locally | |  | No impact has occurred – manage locally |   **Grade**   |  |  | | --- | --- | |  | **Grade** | | **Likelihood** |  | | **Impact** |  | | **OVERALL GRADE** |  |   **RAG Rating**  No impact has occurred – deal with locally  An impact is unlikely – deal with locally  Reportable to the ICO  Reportable to the ICO / DHSC notified |

1. Investigation Findings

The table below lists the investigation findings of the data security incident / breach.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Finding** | **Action Plan** | **Lead** |
|  |  |  |  |
|  |  |  |  |

1. Outcomes

**Staff Outcomes**

The table below details any staff investigations / actions taken as a result of the data security breach / incident.

|  |  |
| --- | --- |
| **Item** | **Details** |
| Have staff been suspended pending results of the investigation? |  |
| What impact has been made on service provision? |  |
| Whether, and to what degree, has any member of staff been disciplined and why? |  |

**Information Commissioner’s Office (ICO) Outcome**

The table below details the enforcement action taken by the ICO regarding the data security breach / incident. Please note this information may be delayed pending the severity of the incident and the ICO’s timescales for replying.

|  |  |
| --- | --- |
| **Item** | **Details** |
| ICO Reference Number for the data security breach / incident |  |
| What action has the ICO taken against the organisation regarding the data security breach? |  |

1. Lessons Learned / Action Plan

The table below lists the lessons learned and action plan in order to mitigate the data security incident / breach occurring in the future.

| **Action Ref** | **Action** | **Lead** | **Details / Update** | **Date Completed** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

END OF REPORT