

Public Service

 **ombudsman**

Data Incident Management Policy

V4 Jan 2026

1 Purpose

- 1.1 Despite our best efforts, things do not always go as planned. When security incidents occur, they can have serious consequences, making it essential that everyone understands how to respond effectively. This policy explains the actions to take in the event of a data security incident.

2 Policy Scope

- 2.1 Everyone who works for or on behalf of us, including employees, contractors, clinical advisers, consultants, and visitors, must understand how to recognise and respond to an incident. This requirement also applies to any organisation that has access to our data and/or systems while providing services on our behalf. Where these organisations process personal data on our behalf, they are known as data processors.
- 2.2 All employees must report any actual or suspected data security incident, breach, or risk that could potentially lead to a data breach to either the DPO or the Privacy, Integrity and Assurance team.
- 2.3 Cyber, information, and security incidents must be reported via HelpHub, which is monitored daily. If the incident is serious or poses an immediate risk, you should also contact a member of the team directly as mentioned above. If you believe someone is in immediate physical danger, call the police without delay.

3 What do you need to report?

- 3.1 All information, cyber, and security incidents must be reported to the Privacy, Integrity and Assurance team via HelpHub. If something does not seem right or gives you cause for concern, you should report it and we will assess the situation and take the appropriate action.

4 What is a security incident?

- 4.1 A security incident is when our people, premises or data are at risk of harm or compromise. Here are some examples: -
 - **Confidentiality of Data:** - Access to personal data, special category data, and other confidential information must be restricted to authorised individuals. Where unauthorised access occurs, whether accidentally or deliberately, this is a data breach and must be reported immediately.

This includes:

- Sending a completed complaint outcome letter to the wrong person.

- Emailing the wrong person and disclosing personal data or special category data relating to another individual.
- Publishing a case summary without fully removing names or other identifying information.
- Attaching the wrong set of medical records to an email.
- Sending the wrong call transcript to a complainant, resulting in the disclosure of information relating to another person's complaint.
- Providing access to confidential information to someone who does not have the authority or business need to view it.

4.2 **Integrity:** - Information must be accurate, complete, and kept up to date as far as reasonably possible. When information is incorrect, incomplete, altered without authorisation, or otherwise compromised, it can lead to a security incident and may affect our ability to deliver its services effectively.

This includes: -

- Failing to keep employee or personal details up to date on HR systems, resulting in correspondence being sent to the wrong address.
 - Inaccurate or incomplete record keeping leading to poor decision-making.
 - Retaining information beyond its approved retention period.
 - Failing to update or correctly record a complainant's address or email address, resulting in important communications not being received.
 - Saving documents to the wrong case file.
 - Producing inaccurate reports or management information based on incorrect or incomplete data.
- **Availability:** - Protecting information from unauthorised access is essential, but it is equally important to ensure that information, systems, and services are available when needed. When information cannot be accessed, recovered, or used in a timely manner, this can result in a security incident and may affect our ability to deliver its services effectively.

This includes: -

- During an emergency, being unable to contact staff to provide important updates or instructions, such as advising them not to travel to an office location.
- Finance systems becoming unavailable, preventing the payment of staff or suppliers and causing personal or commercial disruption.

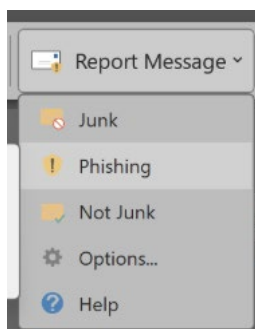
- Accidental deletion of information that is required to be retained.
 - Failure to identify, preserve, and retain material evidence needed for investigations, legal proceedings, or casework that could cause a delay while replacing it.
 - Changes to user account permissions that remove or restrict access to the systems, applications, or information required to perform your role.
 - Loss of access to critical records, documents, or case information when they are needed.
- **Cyber- Attack:** - This occurs when cyber criminals attempt to gain unauthorised access to information, systems, or services, or otherwise disrupt our ability to operate effectively.

This includes: -

- **Phishing attacks:** Emails, messages, or phone calls that appear to come from a trusted organisation or individual and are designed to trick recipients into disclosing information, clicking malicious links, opening harmful attachments, or taking actions that could compromise security.
- **Ransomware attacks:** Malicious software used by cyber criminals to encrypt data or block access to systems and networks. Attackers typically demand a ransom for restoration of access and may threaten to publish, delete, or sell stolen information.
- **Social engineering:** Techniques used by cyber criminals to manipulate individuals into revealing confidential information or carrying out actions that compromise security. This often involves impersonating a trusted colleague, senior leader, supplier, or other legitimate contact and creating a sense of urgency.

5 Phishing Emails

- 5.1 We provide a simple, one-click method for reporting suspicious emails that may be phishing attempts. Colleagues can use the **Report Message** button in Outlook to report suspicious emails directly to the appropriate team for review.
- 5.2 If you receive an email that looks unusual, unexpected, or suspicious, use the **Report Message** button to report it. The same functionality can also be used to report spam or junk emails, helping to protect both you and the organisation from potential threats.



- 5.3 However, if you have clicked on a suspicious link, opened a document, or downloaded an attachment from a suspected phishing email, you must report the incident via HelpHub and contact the Privacy, Integrity & Assurance team immediately. You should also contact the Helpdesk so that your device can be scanned and checked for compromise. In most cases, this can be carried out remotely.

6 What do we need to know?

- 6.1 The more information you provide the faster we can review the breach, consider the risks and access the potential impact.

- 6.2 Here are some key

- When did the breach happen?
 - Date and time also include when did we become aware as we have a limited amount of time to decide if we need to report externally.
- Who caused the breach and or has been involved?
 - The full name of the person/s involved and departments, so we know where to direct any questions to help with the investigation.
- How many data subjects may have been affected?
 - It's important to know if multiple people have been affected, it will potentially escalate the seriousness of the breach.
- What type of data has been breached?
 - It's important to understand the content of the data involved for establishing the potential harm to the subject. Was it limited to a small amount of personal data or was there more sensitive data involved?
- What is the volume of data per data subject?
 - It's helpful to understand the volume of each type of data which may have been disclosed. If we have multiple individuals, was it personal and or special category data for each person?
- Has this been escalated internally? If so who to?
 - Who has been made aware and are there recommendations on what we need to do. It is important to let us know if this has been escalated

to management so we can contact the right people to discuss quickly if needed.

- What steps have been taken to contain the breach?
 - Have we been able to secure the data? If so when and how? If it was an email have they confirmed it has been deleted or have we need able to recall it. If the data was posted have we received it back? Its important to document this where possible.
- Have we contacted the data subject?
 - It's important to know if the data subject/s are aware, if they are not, please seek guidance from the Information Access & Assurance Team before you contact them.
- What system or network has been affected?
 - Is this a technical breach that is impacting one or more of our systems and or the network? Are they core systems that are critical to the organisations function? Are all users impacted or is this isolated to a small group?

7 The Investigation

- 7.1 There is a limited amount of time to report a breach externally, for example the Information Commissioners Office (ICO) expect to be notified of a reportable breach within 72 hours of you being aware. (These are not working hours so include evenings and weekends) The Data Protection Officer and Deputy Director of Legal will decide if we need to report externally and who to.
- 7.2 This means we must assess incidents quickly to determine whether external reporting is required. Where reporting is recommended, the matter must be escalated internally for approval. Every hour is critical, allowing us sufficient time to review the incident, obtain the necessary agreement, establish communication with the relevant external body, and coordinate the next steps.
- 7.3 We will always make every effort to carry out a thorough investigation to understand the potential impact on us and any affected data subjects. However, the extent of the investigation may be limited by the information available and the length of time between the incident occurring and it being reported.
- 7.4 It is vital that the Privacy, Integrity & Assurance Team receives all available information as quickly as possible and is kept updated as the investigation progresses. This information is essential to support the DPO and CDTO in determining whether external reporting is required and whether affected data subjects need to be notified.

- 7.5 A root cause analysis (RCA) will be undertaken to identify the underlying causes of the breach and determine what steps can be taken to prevent a recurrence. This will involve reviewing the circumstances of the incident alongside existing processes, controls, and documented guidance to identify any contributing factors. The findings will then be used to assess whether current arrangements are sufficiently robust or whether improvements can be made to reduce the risk of similar incidents occurring in the future.

8 Escalation

- 8.1 Any data breach that has any of the below factors must be escalated urgently if:
- There is a risk of significant harm to one or more data subjects' rights and freedoms
 - There is a data breach impacting more than 5 individuals
 - A breach involving a large volume of special category data
 - If there is an impact to one of the business-critical system/s
- 8.2 Escalation is to: -
- Data Protection Officer, Alex Daybank
 - Information Access Manager, David Loughlin
 - Information Governance Analyst, Nada Leddy Rouse
 - Information Governance Analyst, Charlotte Carter
- 8.3 Escalation must take place promptly, even where only limited information is available. We do not have to wait for all the facts to be established before reporting the incident. Early notification enables us to assess the risk, begin any necessary investigation, and meet statutory reporting deadlines. Failure to escalate an incident in a timely manner may expose us to significant regulatory consequences and could result in disciplinary action.
- 8.4 Escalation is not simply a tick-box exercise. It provides an opportunity for a contextual discussion about the incident, including any wider considerations such as emerging themes, trends, patterns, or potential organisational risks.

9 External Reporting

- 9.1 In the event of a serious data breach that requires external reporting, the organisation we report to will depend on the nature and circumstances of the incident. Potential reporting obligations may arise with a number of external bodies. The main organisations to which we may be required to report are:
- Information Commissioner's Office (ICO) is the UK's independent body set up to uphold information rights. The ICO can only be reported with authorisation of the Data Protection Officer.

- The National Cyber Security Centre (NCSC) who provides a single point of contact for SMEs, larger organisations, government agencies, the public and departments. We also work collaboratively with other law enforcement, defense, the UK's intelligence, defence and security agencies and international partners.
- The Police may also be someone we have to report to if potentially we think a crime has been committed.

10 Incident Response Group

10.1 The Incident Response Group will be established by the Data Protection Officer (DPO) when a serious incident has been escalated. The group is responsible for decision making, assessing the incident, determining whether external notification is required, and deciding which organisations or individuals need to be informed.

10.2 The Incident Response Group may include: -

- Data Protection Officer
- Deputy Director of Legal (or their representative)
- Assistant Director of the area the breach occurred in
- Senior Information Risk Owner
- Assistant Director of Digital (where incident relates to a DDaT issue or a suspected cyber security event)

10.3 The Incident Response Group will coordinate the organisation's response, including decisions relating to external reporting and the notification of affected data subjects. The Group will also ensure that key internal stakeholders are informed of any decisions made and the actions required.

- Where external notification is being considered, input and approval will normally be required from one or more of the following, as appropriate:
 - Ombudsman
 - Executive Team Member

11 Key Principles

11.1 You can report an incident through the Ombudsman Help Hub. It is important to provide as much information as possible when submitting a report. At a minimum, we need to understand when the incident occurred, who was involved, what happened, and any actions that have been taken since the incident was identified.

- 11.2 If the incident is, or is likely to be, a critical concern, please also refer to a manager and contact a member of the Privacy, Integrity & Assurance Team directly so that we can assess the situation and respond promptly.
- 11.3 We have a legal obligation to report certain personal data breaches to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of them. Its important to report as soon as possible but no more than 4 hours from being aware.
- 11.4 Do not delay reporting an incident while carrying out your own investigation. Even if all the facts are not yet known, report the incident as soon as possible using the information available at the time. Additional details can be provided and the incident record updated as the investigation progresses.

12 Roles and Responsibilities

- 12.1 Managers will take responsibility for ensuring their team complies with this policy.
- 12.2 All employees have a responsibility to ensure that we work as a team and promote awareness and understanding of information security.
- 12.3 Regular training and refreshers sessions will be available, all employees are responsible for keeping up to date with their training via my learning.

Annex A | Assessing severity levels and appropriate response

The following six pages detail the severity level and appropriate response. These levels are:

Level	
SEVERE RISK	Likely to have significant impact on the rights and freedoms of individuals and/or cause mission critical failure.
HIGH RISK	Likely to have limited impact on the rights and freedoms of a small number of individuals and/or cause limited impact on business operations
MEDIUM RISK	Incident has occurred but is limited in impact and scale.
LOW RISK	Incident has occurred but has no risk of causing harm or distress due to mitigating factors.
NEAR MISS	Would have had significant impact on the rights and freedoms of individuals and/or cause mission critical failure except for single mitigating factors or unforeseen development.
NO INCIDENT	No incident has occurred



Assessing Information security incidents **SEVERE**

SEVERE	
Likely to have significant impact on the rights and freedoms of individuals and/or cause mission critical failure.	
Cyber	Security Operations Centre (SOC) response invoked, incident must be reported to NCSC, Police. Full formal investigation initiated directed by DPO reporting to CDTO and AD of Digital. Resulting action plan reported and monitored by ARAC.
Information	Notifiable to the Information Commissioner’s Office (ICO) within 72 hours by DPO. Full formal investigation initiated directed by DPO reporting to CDTO. Resulting action plan reported and monitored by ARAC.
Security	Police, our role to support and provide access to evidence, witnesses etc.

▼ **Assessing Information security incidents** **HIGH RISK**

HIGH RISK	
Likely to have limited impact on the rights and freedoms of a small number of individuals and/or cause limited impact on business operations.	
Cyber	Security Operations Centre (SOC) response invoked, root cause analysis review conducted and action plan agreed. Informal investigation initiated directed by DPO reporting to CDTO. Resulting action plan monitored by DPO and incident response forum.
Information	Informal investigation initiated directed by DPO reporting to SIRO. Resulting action plan monitored by SIRG.
Security	Police Internal informal investigation initiated by security officers reporting to SIRO and CDTO (if appropriate, police may take on all elements of investigation, and our role is limited to providing evidence, access to witnesses etc).

▾ Assessing Information security incidents **MEDIUM RISK**

MEDIUM RISK	
Incident has occurred but is limited in impact and scale.	
Cyber	Investigated by information security team, incident review completed
Information	Informal investigation initiated by DPO reporting to SIRO.
Security	Police Internal informal investigation initiated by security officers reporting to SIRO and DPO (if appropriate, police may take on all elements of investigation and our role limited to providing evidence, access to witnesses etc).

▾ Assessing Information security incidents **LOW RISK**

LOW RISK	
Incident has occurred but has no risk of causing harm or distress due to mitigating factors.	
Cyber	Record, and apply appropriate remediation measures.
Information	Record, and apply appropriate remediation measures.
Security	Record, and apply appropriate remediation measures.

▾ **Assessing Information security incidents** NEAR MISS

NEAR MISS	
Would have had significant impact on the rights and freedoms of individuals and/or cause mission critical failure except for single mitigating factor or unforeseen development.	
Cyber	Security Operations Centre (SOC) response invoked, does not need to be reported further. Full formal investigation initiated directed by DPO reporting to SIRO. Resulting action plan reported and monitored by SIRG.
Information	Full formal investigation initiated directed by DPO reporting to SIRO. Resulting action plan reported and monitored by SIRG.
Security	Not applicable

▾ **Assessing Information security incidents** **NO INCIDENT**

NO INCIDENT	
This is when an incident is downgraded following an investigation or is reported to but not within the control of such as a Trust sending us the wrong information. It is still worth recording as we can include in our feedback activities.	
Cyber	Record, no action but inform Security of OWI/data controller if appropriate
Information	Record, no action but inform DPO of OWI/data controller if appropriate
Security	Record, no action but inform Security of OWI/data controller if appropriate

Version control

Date	Version	Amends	Owner of amends	Approval
10 Aug 2023	2.0	Policy drafted	Nada Leddy Rouse	AD ICT, AD DSP @ TDA 9 August 2023
5 Nov 2024	3	Updates to names, titles, teams and phishing button changes.	Nada Leddy Rouse	Alex Daybank
22 Aug 2025	3.1	Full review, update to job titles and general wording to give more clarity on escalation and reporting.	Nada Leddy Rouse	Alex Daybank

30 Jan 2026	4	Full review with some minor updates. Addition of new section 10 to provide more clarity on decision makers and who needs to be informed when reporting externally.	Nada Leddy Rouse	Alex Daybank
3 Sept 2026	4.1	Changes due to name change, updated to wording	Nada Leddy Rouse	