Parliamentary and Health Service Ombudsman

Security and Information Incident Management Policy

Version 4| January 2026

1 Purpose

1.1 Despite our best intentions, sometimes things don't work out as we planned. When it comes to security incidents, this can have very real consequences so it's important to know what to do when things go wrong. This policy sets out what to do in the event of an information, cyber or security incident.

2 Policy Scope

2.1 Everyone who works for PHSO, including staff, contractors, clinical advisors, consultants, or visitors, needs to know how to respond to an incident. This also applies to any company operating on our behalf that has access to information and or systems. Where these third parties have access to personal data they are known as data processors.

2.2 All PHSO employees are responsible for reporting any data security breach or risk that could potentially lead to a data breach to the Information Access & Assurance team.

2.3 You will need to report cyber, information or security incidents via helphub which is checked daily, if the breach is serious please also contact a member of the team. If you are worried about someone being in physical danger, then immediately call the police.

3 What do we need to report?

3.1 All information, cyber or security incidents need to be reported to the Information Access & Assurance Team via Help hub. Below are some examples but in short, if it feels wrong or concerns you, please report it and the team will assess and respond accordingly.

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. Examples include:

- **Confidentiality of data** | All personal, special category or confidential information should be restricted to authorised individuals only. When someone who isn't authorised gains access, (accidentally or maliciously) this is a data breach.

Examples include:

– Sending a completed complaint letter to the wrong person.

– Emailing the wrong person and disclosing personal or special category data relating to other individuals.

– Publishing a case summary without fully redacting names or other identifying information.

- Attaching the wrong set of medical records to your email.

- Sending the wrong call transcript to a complainant disclosing details of someone else's call about their complaint.

- **Integrity** | Data should always be kept up to date and accurate to the best of our ability. When our data is of poor quality or inaccurate, this can create a security incident.

For example:

– Not keeping personal and employee details up to date on our HR system leading us to send a letter to the wrong address.

– Inaccurate record keeping can lead to poor decision making.

– Keeping information beyond the retention period.

- Failure to update or accurately input a new address or email of a complainant and we send important updates that they do not get.

- Saving the wrong documents to a case file.

- Inaccurate reporting

- **Availability** | We all recognise that it's important to keep information safe and secure from unauthorised access. But just as important is making sure that it's available as and when we need it. Failure to do so could create security incidents like:

– During an emergency, it's important to have access to contact all our staff, for example to warn them not to travel into the office.

– If the finance system is unavailable, we may not be able to pay our staff or suppliers, leading to personal or commercial difficulties.

– If we mistakenly delete data that needs to be retained

- Failure to mark and retain material evidence

- Change in permissions on your account that remove your ability to access the systems and data you need to do your job

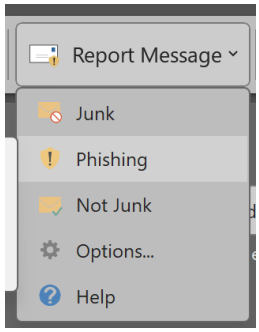
- **Cyber-attack |** This is when criminals attack PHSO to gain unauthorised access to our information or to compromise our ability to do our jobs. Common cyber-attacks include:

    - Phishing attacks: when someone sends an email pretending to be from a legitimate company or person to con the recipient into doing something that could cause harm.
    - Ransomware attacks: when criminals lock people out of their systems and networks, only allowing access once a ransom has been paid. Often threatening to delete or leak data to the public.
    - Social engineering: in which criminals use human behaviors to manipulate someone to divulge confidential or personal data. Often posing as someone high up within the organisation asking for urgent action like paying an invoice.

5 Phishing emails

5.1 PHSO has introduced a one-click approach to reporting suspicious emails that maybe be phishing. PHSO colleagues can use the 'Report Message' button to report suspicious emails directly from outlook.

If you notice something that doesn't look right use the button to report. We also have the feature to report spam/junk mail.



5.2 However if you have inadvertently clicked on a phishing link, document or downloaded an attachment from a suspicious email, please report to helphub and contact Information Access &

Assurance Team. Your device will need to be scanned (this can be done remotely) so you will also need to contact the Helpdesk.

6 What do Information Access and Assurance need to know?

6.1 The more information you provide the faster we can review the breach and potential impact.

Here are some key bits of information that will be helpful to the investigation: -

- When did the breach happen?
  - Date and time, also include when we became 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?
  - Its 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 breach 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 requires us to review the incident quickly to determine if we need to report externally. If we recommend reporting it must be escalated internally to be agreed. So, every hour counts to ensure we can review, escalate, and formally establish communication to the external body and next steps.

7.3 We will always do everything possible to carry out a full investigation to understand the potential impact on PHSO and the data subject/s involved. This can be limited based on what information is available and the time between the incident and when it is reported.

7.4 It is vital that the Information Access & Assurance team are provided with as much information available promptly and updated as the investigation develops. The Data Protection Officer and Deputy Director of Legal will require this to make the decision on external reporting and whether we need to inform the data subjects.

7.5 A root cause analysis (RCA) will be completed to understand what caused the breach and if changes can be made to prevent it happening again. We will review the current processes and documented guidance against what happened to determine what factors contributed to the breach. Once completed we can consider whether the process and documentation are robust enough or can changes improve the process to reduce the risk of recurrence.

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 Security Analyst, Nada Leddy Rouse

8.3 Escalation must be timely, even if there is limited information initially, just contact with what we know so far. Failure to escalate can incur considerable penalties for PHSO and may result in disciplinary action.

8.4 Escalation is not about a tick box exercise, it's about having a contextual discussion and working through any additional considerations such as emerging themes and trends.

9 External reporting

9.1 In the event we suffer a serious data breach that we need to report externally. Depending on the nature of the data breach will determine who we should be reporting to. The main external bodies we may report to 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, defence, the UK's intelligence 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 DPO when a serious incident has been escalated. It is responsible for the decision making on whether external notification is required and if so who is notified.

10.2 The Group will be 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 Group will coordinate the response actions, specifically regarding external reporting and notifying data subjects, and inform key internal stakeholders of the decision and actions to follow. External notification will usually require input and agreement from at least one of the following:

- Ombudsman (if appropriate)
- Executive Team Member (if appropriate)

11 Key Principles

11.1 You can report an incident using the Ombudsman help hub, it is important to provide as much detail as possible. We ideally need to know when it happened, who has been involved and what has happened since.

11.2 If potentially it is a critical concern, please also contact a member of the team directly to discuss so we can respond promptly.

11.3 We have 72 hours to report serious data breaches to the ICO, so it is important to report to Information Access & Assurance team as soon as possible. Ideally as soon as it has been discovered but no more than 4 hours from being aware so we can investigate.

11.4 It is important not to delay reporting while you investigate, even if we do not have all the information, please report with what you know so far. We can update the incident 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 on help hub.

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 PHSO 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, PHSO 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 PHSO role 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 directed 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 PHSO 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 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 PHSO 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

Version	date	Changes	Agreed By
2	10/8/2023	Policy Created	AD ICT, AD DSP @ TDA 9 August 2023
3	5/11/2024	Updates to names, titles, teams and phishing button changes.	NLR -Minor updates only
3.1	22/8/2025	Full review, update to job titles and general wording to give more clarity on escalation and reporting.	NLR -Minor updates checked with AD
4	30/1/2026	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.	NLR - updates approves with AD