# Information Security Breach Policy

**Title:** Information Security Breach Policy  
**Original Author(s):** Information and Records Manager  
**Owner:** SIRO  
**Reviewed by:** Security and Information Assurance Committee  
**Quality Assured by:** Director of Operations  
**Meridio Location:** To go in 1.07 APPROVED STRATEGIES, POLICY AND GUIDANCE / Business Policy and Guidance  
**Approval Body:** Executive Team  
**Approval Date:** 07/10/2014

## Change History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Status</th>
<th>Update by</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>01/10/13</td>
<td>To be approved</td>
<td>Katharine Stevenson</td>
<td>In draft; shared with LIRAs and SIAC. QA by Frank Garofalo and Helen Hughes.</td>
</tr>
<tr>
<td>1.0</td>
<td>08/10/13</td>
<td>Approved</td>
<td>Katharine Stevenson</td>
<td>Approved by Leadership Team</td>
</tr>
<tr>
<td>1.1</td>
<td>20/02/14</td>
<td>To be approved</td>
<td>Katharine Stevenson</td>
<td>Updated following recommendations from Internal Audit report. Submitted to Executive Team</td>
</tr>
<tr>
<td>2.0</td>
<td>22/01/15</td>
<td>Approved</td>
<td>Hannah Burling</td>
<td>Approved by Executive Team 07/10/14</td>
</tr>
</tbody>
</table>
1. Purpose

1.1 The Parliamentary and Health Service Ombudsman holds a lot of information. Care is always taken to protect our information assets and avoid an information security breach. In the unlikely event of information being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

1.2 This policy sets out the responsibilities of PHSO staff and contractors in any situation where information has been lost, stolen or passed onto or accessed by an unauthorised person or organisation. This is known as an information security breach.

1.3 This policy includes details on PHSO’s threshold for reporting Data Protection breaches to the Information Commissioner’s Office (ICO). It also confirms that only the Head of Information and Records Management (or their deputy) is permitted to notify the ICO of Data Protection breaches, with the approval of the Senior Information Risk Owner (SIRO).

2. Scope

2.1 This policy applies to all information assets held by PHSO, regardless of format. It encourages a risk-based and proportionate approach to handling information security breaches. PHSO evaluates all information security breaches on a case-by-case basis and makes decisions on actions according to the assessment of risks in the particular circumstance.

3. Introduction

3.1 The Data Protection Act 1998 (DPA) makes provision for the regulation of the processing (use) of information relating to individuals, including the obtaining, holding, use or disclosure of such information. Principle 7 of the DPA states that organisations which process personal data must take “appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data”.

3.2 PHSO is also committed to achieving the required standard of information security under the Government’s Information Assurance Maturity Model (IAMM). This model is aimed at reducing the risks posed to our information assets as we use and share information. This policy will help PHSO to manage situations where information use and sharing has gone wrong, in a proportionate and effective manner.

3.3 As well as the reasons given under the DPA and IAMM, any information security breach can have a negative impact on the PHSO’s reputation and the public perception of us as a trustworthy organisation. Not all incidents result in personal data breaches, and not all breaches require notification to the ICO,
some may involve loss of our financial or operational information. This policy is to ensure that regardless of the incident type, PHSO has a consistent and proportionate approach to handling information security incidents.

4. Types of Information Security Breach

4.1 Information security breaches can be caused by a number of factors. For example:

- Lost or stolen laptops, removable storage devices, BlackBerry devices, or paper records left in public areas (i.e. trains)
- Hard disk drives and other digital storage media (integrated in other devices such as multifunction printers) being disposed of or returned to suppliers without the contents first being deleted
- Databases and systems being ‘hacked’ into or otherwise illegally accessed by individuals outside the PHSO
- Paper records lost or stolen from insecure recycling
- PHSO mistakenly providing information to the wrong person, or organisation for example by sending details out to the wrong address, email or fax number
- An individual deceiving the PHSO into improperly releasing the personal information of another person (including by telephone)
- Unforeseen circumstances such as fire or flood
- Not applying the Protective Marking scheme and handling arrangements correctly.

4.2 In order for an incident to be considered a breach under the DPA, it must contain personal information.

5. Preventing information security breaches

5.1 All staff are responsible for protecting our information assets from misuse, loss or unauthorised access, modification or disclosure. This does not mean that information cannot be used or shared, but that appropriate steps must be taken to ensure that information is protected in the process. All staff are expected to attend training relating to information security, and should read and apply the protective marking scheme and handling arrangements outlined in the Security Guidance to ensure they are using and sharing information appropriately. The FOI/DPA team can advise further on which information can be shared externally.

5.2 PHSO is required to take reasonable steps to protect the personal information we hold. Where the ICO finds significant failings in protecting personal information, a fine of up to £500,000 can be levied on any organisation. All staff are therefore expected to take responsibility for personal data in their care by following internal policies and guidance relating to information security. Failure to do so may result in disciplinary action. Annex A provides further details on how staff can help to avoid information security breaches.
6. Recognising an information security breach, or potential breach

6.1 The first questions you should consider when assessing whether there has been an information security breach are: is the information missing or has it been sent to the wrong person? If you can answer yes to one or more of the above questions then you have identified a potential data breach.

6.2 If you believe a document or file is missing internally, please ensure that you carry out a search of all cupboards, pedestals and storage before following the next steps. Use the guidance provided in annex B.

7. Reporting and risk assessment

7.1 Once an information security breach has been identified it must be reported to your line manager and the Head of Information and Records Management or their deputy. If the breach occurs outside normal working hours, this should begin as soon as is practicable.

7.2 Please provide as much detail as possible when reporting a breach, for example:

- Case reference number and name (if casework)
- History Item numbers or links to documents saved in Meridio that have been compromised
- Summary of how the breach occurred or was discovered
- Whether a complainant or stakeholder has expressed their concern in the incident
- What steps have you taken to mitigate the risk? i.e detail what searches you have carried out or whether you have reported the theft of personal belongings to the police?

7.3 The Head of IRM must use the information provided to carry out an assessment of the information security breach by completing an Information Security Breach Assessment form (see Annex C) and save it in section 3.03 BUSINESS SECURITY / BUSINESS SECURITY INCIDENTS, and record it on the security log.

7.4 The assessment takes into consideration the following:

- the type of information involved, in particular its sensitivity
- whose information was involved
- the detrimental impact on any individuals or organisations
- what protections were in place (i.e. encryption)
- what has happened to the information
- whether the information could be put to any illegal or inappropriate use
- whether it breaches any of the data protection principles
7.5 If the overall risk is assessed as **High**, the Head of IRM must request their Executive Director to notify the SIRO of the incident. The Security Officer must also be informed.

7.6 If the overall risk is assessed as **Medium**, the Head of IRM must notify their Executive Director of the incident, with a view of discussing whether the SIRO should also be informed. The Security Officer must be informed of any incidents reported to the SIRO.

7.7 If the overall risk is assessed as **Low**, the Head of IRM can continue to handle the incident locally. The incident will be summarised in a monthly report sent to the SIRO, Information Asset Owners and the Security Officer.

7.8 The IT Security Officer must always be informed of any incidents involving lost, stolen or hacked IT equipment, or if a break-in has occurred.

7.9 All incidents will be summarised in monthly reports to the SIRO and Information Asset Owners, and in quarterly reports to the Leadership Team which will also be shared with the Security and Information Assurance Committee.

7.10 A decision to report a data protection breach to the ICO will be made by the SIRO using the evidence and assessment collated by the Head of IRM. The Head of IRM is the only person in PHSO who is permitted to report data protection breaches to the ICO, with the approval of the SIRO or in their absence, the Executive Director of Operations and Investigations. In the absence of the Head of IRM, the Information Records Manager will report a data protection breach to the ICO.

8. **Mitigating actions**

8.1 Following the assessment, the Head of IRM (or SIRO if escalated) will take appropriate steps to recover any losses and limit the damage. Steps might include:

- Attempt to recover lost equipment or information
- Ascertaining whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system.
- Contact relevant teams so that they are prepared for any potentially inappropriate enquiries ‘phishing’ for further information on the individual concerned. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer’s name and contact details if possible and confirm that they will ring the individual making the enquiry back. Whatever the outcome of the call, it should be reported immediately to the relevant manager.
- Consider contacting the External Affairs Team so that they can be prepared to handle any press enquiries. The SIRO will need to clear any press lines.
- Investigate the use of back-ups to restore lost/damaged/stolen data.
- If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
• If the data breach includes any entry codes or passwords, then these codes must be changed immediately
• In the most serious cases, consider contacting the police (Security Officer, with approval of SIRO)
• Consider informing the person or organisation involved. When notifying individuals, give specific and clear advice on what they can do to protect themselves and what you are willing to do to help them. They should also be given the opportunity to make a formal complaint if they wish (see the PHSO’s Complaints Procedure)
• Consider the use of appropriate capability/disciplinary action
• Report the incident to the ICO (Head of IRM, with approval of SIRO)

8.2 The actions must be recorded in the Information Security Breach Assessment Form (Annex C) by the Head of IRM or their deputy.

9. Review and Evaluation

9.1 Following the assessment and mitigating actions, the Head of IRM must review the causes of the breach and recommendations for future improvements should be made and recorded on the Information Security Breach Assessment form. The lessons learned must be shared with the appropriate individuals, including the relevant Information Asset Owner.

9.2 If systemic or on-going problems are identified, then an action plan must be drawn up to correct these. If the breach warrants a disciplinary investigation, the Head of IRM should liaise with Human Resources and the manager for advice and guidance.

10. Monitoring and Compliance

10.1 Monthly summaries of information security incidents will be shared with the SIRO, Information Asset Owners and Security Officer.

10.2 Quarterly reports on information security incidents will be presented to Leadership Team and the Security and Information Assurance Committee.

10.3 Annual assurance on Information Security will be given at the end of the business year.

11. Roles and Responsibilities

11.1 All PHSO staff have a responsibility to ensure that our information is used and shared appropriately and in line with the Security Guidance. Different staff however have different roles in relation to information security and these responsibilities are outlined below:

The Ombudsman: Has a duty to ensure that her Office complies with the requirements of the Data Protection Act and supporting regulations and codes in information security. It is the intention of the Ombudsman that PHSO
delivers an exemplary standard of information and records management, including information security.

**Senior Information Risk Owner (SIRO):** Will act as an advocate for information risk. They are the representative at the PHSO Board, Audit Committee and Leadership Team who understands the strategic business goals of the PHSO and how these may be impacted by the failure of information assets. The SIRO is responsible for ensuring that management of information risks are weighed alongside the management of other risks facing the organisation such as financial, legal and operational. The SIRO is responsible for the decision to report a data protection breach to the ICO.

**Leadership Team:** Will review quarterly Information Governance reports which include details of Information Security and provide feedback.

**Information Asset Owners:** Responsible for the security of their information assets, helping the Head of IRM to coordinate responses and mitigations to information security incidents.

**Head of Information and Records Management:** Is responsible for the management of this policy and its supporting procedures, including completing Information Security Breach Assessments and escalating to the SIRO through their Executive Director when necessary. The Head of IRM is the only person in PHSO responsible for reporting data protection breaches to the ICO, with the knowledge and approval of the SIRO.

**Information and Records Manager:** Acts as a deputy for the Head of IRM.

**Security Officer** Responsible for the overall security of PHSO’s assets, including information. In their dual role as Head of ICT and IT Security Officer they maintain the technology used for storing PHSO’s information assets, ensuring that confidentiality, integrity and availability of information is maintained at all times.

**Security and Information Assurance Committee:** provides feedback on incidents reported and assistance in communicating messages

**All staff:** Responsible for looking after our information assets in accordance with PHSO’s Security Guidance. They are also responsible for reporting incidents when they occur and assisting the Head of IRM with their assessment.

### 12. Implementation

12.1 This policy takes effect immediately. All managers should ensure that staff are aware of this policy and its requirements. This should be undertaken as part of induction. If staff have any queries in relation to the policy, they should discuss this with their line manager or the Head of Information and Records Management.

12.2 This policy will be reviewed every three years unless required sooner by legislative changes, new case law or new guidance.
13. Annex A - Help to avoid information security breaches

We are all responsible for helping to protect the information we create and receive. While most of the personal data we collect is through our casework, we may collect personal data as a result of stakeholder events, recruitment, procurement or other PHSO activities. We also generate and receive information through other activities such as in Finance, or Procurement. The list below gives just some of the things you should be doing to help protect the information we hold:

- Double check addresses (email or postal) before sending information out (i.e. ask the complainant to confirm their address)

- Follow the guidance given in the Protective Marking Scheme and Security guidance

- Always check that you are sending the correct documentation when posting information (i.e. check you haven’t left a page on the printer, or likewise picked up someone else’s letter)

- Always update the file holder field on Visualfiles when passing on a case file to another member of staff

- Use a lockable bag or case to transport sensitive documentation. These are available from Business Managers. Do not place bags in overhead shelves on trains or planes, keep bags containing personal or sensitive information with you at all times.

- Avoid discussing or reading about individuals (complainants or staff) in open areas, particularly on trains

- Follow the clear desk policy
14. Annex B - Initial searches for ‘missing’ files

There are bound to be occasions where files, specifically case files, cannot be easily found because someone has forgotten to update the file holder field in Visualfiles. The following is intended to act as a common sense guide in trying to locate missing files.

What is missing?
First, identify what exactly is missing. For example, is it the entire case file or part of it, such as the evidence file?

Who had it last?
Start the search by finding out who last had the case file. There are some obvious questions that can help you find the case file quickly:
- Who is the case file allocated to? Check when they had it last.
- Who made the last ‘history item’ on Visualfiles? Ask them if they have the case file.
- Does anything in Visualfiles indicate where the file might be?

Where is it likely to be?
More often than not, the case file tends to be located with the team. The best chance of recovering the case file quickly is if a very thorough search is carried out within the team. Everyone in the team should be involved, including the line manager, to help ensure that no areas are left unsearched. Key areas to check include:
- Post in / out tray
- Storage Wall(s)
- Low level storage units(s)
- Desks
- Fire Safe(s)
- Pedestals
- Document log

Carrying out a worthwhile search
The search is more likely to be successful if everyone on the team searches at the same time. It is also worth considering asking staff to swap work areas so they search somewhere other than their own desks.
Key things that can help are:
- Search methodically
- Don’t forget people who are on leave etc
- Untie and check each folder in a case file
- Open all TNT boxes and check the contents thoroughly.
Who else might have it?
If you do not locate the file consider if the case file could have been sent elsewhere. Such as:

- Information and Records Management team
- Review team
- Executive Office
- Executive Director / Director
- Clinical Advice
- Legal team (including DP/FOI team)
- Reporting, editing and proofreading team

If it is possible one of the above might have the case file, contact them to check.

Next steps

Once you have done all this, if you are still unable to locate the case file, contact the Head of IRM to report it missing and for further advice. When reporting the incident you should provide as much detail as possible about the searches you have already carried out so that searches are not duplicated.
15. Annex C - Information Security Breach Assessment Form
(To be completed by the Head of IRM only)

Security Incident Log Reference Number:

Security Incident Handler:

Part A: Background

Summary of the incident

Part B: Details of Missing Assets

Any assets, including information, that are missing must be listed here in full. This should include all asset numbers, full description of the asset, serial numbers and details of the information it contained.

<table>
<thead>
<tr>
<th>Description of Asset</th>
<th>Description of Information Contained</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Part C: Risk Assessment

Using the information provided in Parts A and B, the checklist in Annex A and the ICO reporting threshold guidance in Annex B, outline your assessment of the risks and proposal for next steps here. Also include whether the SIRO, External Affairs and Information Commissioner need to be informed.

Part D: Mitigating Actions

All actions taken to contain and recover the missing assets and data must be recorded here. Dates must be given and names of members of staff undertaking actions must be used.

<table>
<thead>
<tr>
<th>Date</th>
<th>Actions taken</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Part E: Review and Evaluation

Review how the data breach occurred, what lessons can be learned and whether any further action needs to be taken for avoiding the mistake in the future.
**Annex A - Risk Assessment Checklist**

Use this checklist as part of your assessment in Part C.

*Some generic risks have been identified already, but this is not a definitive list. Risks can be added to or deleted dependant on the circumstances.*

Answer each of the questions by ticking the relevant box. *In the final box ‘Overall rating’ put the level that most commonly appears. Ie if the majority of ticks are against the Medium level, write medium.*

<table>
<thead>
<tr>
<th>Factor</th>
<th>Answer</th>
<th>Level (H/M/L)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>How the loss occurred</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System hacked</td>
<td></td>
<td>H</td>
</tr>
<tr>
<td>Data was targeted</td>
<td></td>
<td>H</td>
</tr>
<tr>
<td>Device / file stolen</td>
<td></td>
<td>H</td>
</tr>
<tr>
<td>Device / file lost externally</td>
<td></td>
<td>M</td>
</tr>
<tr>
<td>Device / file damaged</td>
<td></td>
<td>L</td>
</tr>
<tr>
<td>Device / file misplaced internally</td>
<td></td>
<td>L</td>
</tr>
<tr>
<td><strong>Volume of data affected</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Significant volume (i.e. more than a dozen case files)</td>
<td></td>
<td>H</td>
</tr>
<tr>
<td>Medium volume (i.e. a couple of case files)</td>
<td></td>
<td>M</td>
</tr>
<tr>
<td>Small volume (i.e. 1 case file)</td>
<td></td>
<td>L</td>
</tr>
<tr>
<td><strong>Data elements breached</strong></td>
<td></td>
<td>(a combination of identifying information should always be considered a high risk with a high likelihood of harm occurring)</td>
</tr>
<tr>
<td>PHSO Case file</td>
<td></td>
<td>H</td>
</tr>
<tr>
<td>Financial account numbers</td>
<td></td>
<td>H</td>
</tr>
<tr>
<td>PIN for financial account</td>
<td></td>
<td>H</td>
</tr>
<tr>
<td>Information belonging to a 3rd party</td>
<td></td>
<td>H</td>
</tr>
<tr>
<td>Protectively marked PHSO information</td>
<td></td>
<td>H</td>
</tr>
<tr>
<td>Sensitive data (as defined by DPA)</td>
<td></td>
<td>H</td>
</tr>
<tr>
<td>PHSO Employee file</td>
<td></td>
<td>M</td>
</tr>
<tr>
<td>Date of Birth</td>
<td></td>
<td>M</td>
</tr>
<tr>
<td>NI / NHS / Passport</td>
<td></td>
<td>M</td>
</tr>
<tr>
<td>Information about private aspects of a person’s life (that doesn’t fall under the DPA definition of sensitive data)</td>
<td></td>
<td>M</td>
</tr>
<tr>
<td>Name</td>
<td></td>
<td>L</td>
</tr>
<tr>
<td>Address, Telephone number, email address</td>
<td></td>
<td>L</td>
</tr>
<tr>
<td><strong>Ability to access the data - the likelihood the personal information will be or has been compromised - made accessible to and usable by unauthorized persons</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paper records in unlocked bag / cupboard off site</td>
<td></td>
<td>H</td>
</tr>
<tr>
<td>Electronic records not encrypted</td>
<td></td>
<td>H</td>
</tr>
<tr>
<td>Email / letter sent to wrong address</td>
<td></td>
<td>H</td>
</tr>
<tr>
<td>Electronic records that are password protected only</td>
<td></td>
<td>M</td>
</tr>
<tr>
<td>Paper records in unlocked cupboard on PHSO premises</td>
<td></td>
<td>L</td>
</tr>
<tr>
<td>Electronic records that are encrypted</td>
<td></td>
<td>L</td>
</tr>
<tr>
<td><strong>Ability to mitigate the risk of harm</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No recovery of data</td>
<td></td>
<td>H</td>
</tr>
<tr>
<td>Partial recovery of data</td>
<td></td>
<td>M</td>
</tr>
<tr>
<td>Recovery of data prior to use</td>
<td></td>
<td>L</td>
</tr>
<tr>
<td><strong>Evidence of data being used for identify theft or other harm</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data published on the web</td>
<td></td>
<td>H</td>
</tr>
<tr>
<td>Data accessed but no direct evidence of use</td>
<td></td>
<td>M</td>
</tr>
<tr>
<td>No tangible evidence of data use</td>
<td></td>
<td>L</td>
</tr>
<tr>
<td>Overall rating</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

13 of 16
**Impact Rating**

Now use the below table to assess the impact or harm to an individual or our organisation:

For example, if a case file containing sensitive witness protection scheme information is lost tick ‘High’. If it is a case file containing medical records for a broken leg, tick ‘Medium’. For sensitive medical issues such as mental illness you may wish to consider a High impact rating.

<table>
<thead>
<tr>
<th>Impact Rating</th>
<th>Impact Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Breach may result in an individual’s injury/death, identity theft, financial loss, and give rise to harassment or prejudice. Breach may result in serious questions being raised about the PHSO’s trustworthiness</td>
</tr>
<tr>
<td>Medium</td>
<td>Breach may result in the individual’s embarrassment, inconvenience or reputation. Breach may result in the individual’s trust in the PHSO</td>
</tr>
<tr>
<td>Low</td>
<td>Breach may result in the individual being concerned that their data could have been potentially miss-used.</td>
</tr>
</tbody>
</table>

**Assigning a Risk Score**

The risk score is determined by cross-referencing the type of breach score with the impact score:

<table>
<thead>
<tr>
<th>Type of Breach</th>
<th>Impact</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td></td>
</tr>
</tbody>
</table>

**High** = Notify the SIRO, consider notifying ICO (if personal data) and individual/organisation involved;

**Medium** = Consider informing the SIRO but handle the incident locally

**Low** = Head of IRM to handle the incident locally

**Overall Score:**

*Examples:*

- If the Type of breach came out as Medium, and the Impact Rating came out as Low the overall score is Low.

- If the Type of breach came out as High, and the Impact Rating came out as Medium, the overall score is High.

**Annex B – ICO reporting threshold**

The following guidance should be referred to when assessing whether the ICO needs to be informed of a personal data breach, and in completing part C of the Information Security Breach Assessment Form. The guidance has been developed from discussions with the ICO and by referring to the ICO Data Protection Regulatory Action Policy for an understanding on the ICO reporting threshold.
The ICO Data Protection Regulatory Action Policy confirms that it is not necessary or proportionate to inform them of all personal data breaches. Providing we take our responsibilities under the DPA seriously and always act to resolve data breaches locally, the ICO is only interested in being told about the most serious incidents, or where trends or reoccurring incidents occur in PHSO.

In deciding the seriousness of a personal data incident, the ICO is keen to emphasise that we should always take into consideration other elements involved in the personal data breach. For example, we must consider:

- **The document type:**
  - Standard template letters and acknowledgment letters are unlikely to hold significant amount of personal data, possibly just name and address.
  - Letters revealing a lot more information other than name and address may have more of a detrimental impact.

- **The detrimental impact:**
  - Some categories of information are likely to have higher harm/distress such as adoptive/foster information; serious health information; criminal records; information relating to vulnerable children/adults; information revealing sexual abuse, domestic violence or child neglect.
  - Consider: will the person be embarrassed, harmed, financially impacted by someone else knowing their personal data, misused or their data being inaccurate?
  - Incidents with a high detrimental impact often feature in incidents where fines have been given.

- **The volume affected**
  - The higher the volume, the more serious it should be treated
  - But still take into consideration the detrimental impact for lower volumes

- **The publicity** given to the breach i.e. has the breach been picked up by the Press or put up on social media sites (report if it has)

- **The cause**
  - Was it human error where despite the policies and procedures, training and systems in place to avoid the mistake, the breach still took place despite the best intentions of the organisation in avoiding it.
  - If it was human error caused because there wasn’t a process or system in place, or because the person hadn’t been trained or aware of their responsibilities, this is more serious.

- **Is there a pattern?**
  - Are the same breaches occurring?
  - When reporting, it is a good idea to inform the ICO of the previous incidents and what we did to mitigate or learn from them, so that they can take that into consideration.
• What remedial action was taken?
  o If we have done nothing, or are unable to prevent further breaches of a similar kind, or if we are unable to retrieve the lost data then we should see that as a more serious issue.