# Data Breach Notification Policy

October 2021

| Document title |
| --- |
| Data Breach Notification Policy October 2021 |
| **Document author and department** |
| Samantha Hill, Data Protection Officer |
| **Approving body** |
| Executive Director of Corporate Governance |
| **Date of approval** |
| 20 September 2021 |
| **Review date** |
| July 2024 |
| **Edition no.** |
| 2 |
| **ID Code** |
| 213 |
| **Date of effect** |
| 1 September 2021 |
| Public access online (internet) and Staff intranet **YES** |
| Public access on request copy to be mailed **YES** |
| External queries relating to the document to be referred in the first instance to the Corporate Governance team:<br>email corporate-governance@port.ac.uk<br>If you need this document in an alternative format, please email corporate.communications@port.ac.uk |

The latest version of this document is always to be found at:

policies.docstore.port.ac.uk/policy-213

# Summary

## What is this document about?

This policy provides a framework for recognising, investigating, reporting and resolving a data security breach.

## Who is this for?

This Policy applies to all members of staff including honorary and visiting staff and governors, as well as students and other individuals who either process personal data within, or on behalf of, the University, or whose personal data is processed by the University. It will also be of interest to the wider public in relation to how the University handles reports or data breaches.

## How does the University check this is followed?

Information Governance staff make information about data protection available on the University website and intranet, and by training staff on data protection principles with examples of good practice. The University encourages staff to raise questions about data protection matters and to report any issues or data breaches they may come across in their work. From the receipt of reports of data breaches, the take up of training opportunities, the knowledge shown by staff and the questions asked, the University believes the policy is being followed.

## Who can you contact if you have any queries about this document?

All enquirers may contact the University's Data Protection Officer, Samantha Hill, on 023 9284 3642 or data-protection@port.ac.uk .

# Data Breach Notification Policy

## 1. Purpose

The purpose of this policy is to:

- Define the term 'personal data breach'
- Describe the data which is at particular risk
- Detail the actions to be taken in the event of a personal data security breach
- Identify those individuals that should be involved in handling a data security breach
- Detail the actions that the University should take to resolve the breach.

## 2. Responsibilities and ownership

2.1 Responsibility for reviewing and updating this Policy lies with the member of the University Executive Board in charge of security and Information Services matters. This responsibility is delegated to the University's Data Protection Officer.

2.2 All members of staff including honorary and visiting staff and governors have a responsibility for the security of the data held by the University and therefore must be aware of, and comply with, this Policy in the event of a personal data breach.

## 3. Definitions

## 3.1 Personal data breach

A personal data breach is a security incident which results in the loss, alteration, compromise, unauthorised disclosure of, destruction or access to, personal data held by the University. The breach may be accidental or deliberate, and is regardless of the format in which the data is held.

### *3.1.1 The detrimental impact of a personal data breach*

A personal data breach may cause significant detrimental impact or embarrassment to the University, including to individuals working or studying at the University or to third parties working with the University.

A personal data breach could affect academic standing, organisational reputation, individual privacy, a risk to individual's rights and freedoms and result in a fine from the Information Commissioner's Office (the Supervisory Authority for the data protection legislation).

## 3.2 Information at particular risk

The following types of information must be kept securely and if lost, damaged or compromised, would constitute a personal data breach:

- Personal data about staff, students or third parties
- Special category data about staff or students
- Financial data about staff, students or third parties
- Commercially sensitive information
- Information exempt from disclosure under the Freedom of Information Act 2000, the Environmental Information Regulations 2004, the General Data Protection Regulation and related data protection legislation.

### 3.2.1 *Personal data about staff, students or third parties*

Personal data is defined as any information that can identify a living individual. These individuals include applicants, staff, students, alumni, business partners and other third party contacts that have provided their personal details to the University. The mere mention of someone's name in a document, for example, as a record of attendance at an open meeting, is not enough in itself to make the information in that document personal data, but this, when combined with other information about an individual could make that information personal data. It is important to remember that personal data is not simply basic details such as name and address, but can also be an expression of an opinion about an individual or an indication of the intentions of any person towards that individual. An individual can also be identified by a combination of details that might not include their name, for example circumstances of an event plus an ID number. Therefore, the definition of personal data is extremely wide.

Examples of personal data held by the University include, but are not limited to:

- The contents of an individual student / staff file
- A staff appraisal assessment
- Name, address, home phone number
- Unique identifying numbers and further linked personal data
- Details about lecture attendance, course work marks and grades
- Notes of personal supervision, including matters of behaviour and discipline
- IP addresses

### 3.2.2 *Special category data about staff or students*

Personal data becomes **special category data** if it includes any of the following types of information about an identifiable, living individual:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Physical or mental health
- Sexual life and orientation
- Genetic and biometric data (used to identify an individual)
- The commission or alleged commission of offences (see DPA 2018 s11)

Special care must also be applied to any data which if lost, whilst not included in the definition of special category data in the General Data Protection Regulation and related data protection legislation, could still be considered to be sensitive, or could lead to theft or identity fraud (e.g. payroll data, personal financial data, SFE (Student Finance England) uploads).

### 3.2.3. *Volume of data lost*

Although there will be a greater risk of harm to the rights and freedoms of individuals if a large volume of personal data is involved, as the 'test' of whether a data breach should be notified to the ICO is the level of risk to the data subject, it may be necessary to notify a breach relating to one individual if their entire record is lost and cannot be recovered. In cases where there is a real risk of individuals suffering harm, then the loss must be regarded as serious and must be reported to the Information Commissioner's Office (ICO). There is no specific guidance as to what constitutes a "large volume" of personal data – each case must be considered on its own merits, as it is the risk to the rights and freedoms of the individuals whose data is involved in the breach that is paramount. For instance, the loss of a small number of records containing special category data would constitute a greater risk to an individual's rights than the loss of a staff telephone directory containing the names and work telephone numbers of over a thousand members of staff.

# 4. Related policies

This policy should be read in conjunction with the following policies

ICT Acceptable Use policy

Data Protection Policy

Records Management policy
Information Security policy

# 5. What to do if you discover or suspect a data security breach

## 5.1 Who to contact

The University has 72 hours from the discovery of a suspected/ actual breach to declare the personal breach to the ICO, therefore staff must act quickly once it is believed a suspected / actual breach has occurred. Anyone who identifies or suspects a personal data breach has occurred should contact the University's Data Protection Officer in the first place. If this individual is not available, please contact either the Information Security Architect in Information Services or the Executive Director of Corporate Governance. If a member of staff is in any doubt about what to do, they should contact the Security Architect or the Data Protection Officer for advice.

## 5.2 What information to provide

You will be asked to complete a data security breach form available here but the information that it is necessary to provide is listed below:

- When the data security breach happened or is thought to have happened
- The actual nature of the breach, e.g. whether computer equipment has been stolen, misuse of log-in, paper files gone missing, data sent to the wrong person.
- Details of the data subject(s) affected, that is, the person/people to whom the data refers
- The nature and quantity of the data believed to have been involved in the breach e.g. whether personal, financial or otherwise sensitive
- Where the breach occurred e.g. in an email, an open office, as part of a University system
- Details of any security employed to a) reduce the risk of a breach occurring in the first instance and b) that will mitigate the risk e.g. encryption of electronic data
- Details of anyone else who may know about the alleged / actual breach.

# 6. What happens next?

The Data Protection Officer and / or the Security Architect will review the information and take the following actions where appropriate:

i) In a *straightforward case* where there is little risk of any harm to the rights and freedoms of the individual, (for example, where an email containing personal data is sent to the wrong individual) the person identifying the breach will be asked to ensure that the person receiving the data incorrectly has been contacted and asked to either delete or return the data, and to confirm that they have taken this action. If this is accomplished, there will be no need to notify anyone further of the incident but the Data Protection Officer will complete a data breach decision notice to record the actions taken and the decision on notification. If it is not possible to obtain confirmation that the data has been deleted, it will be necessary for the Data Protection Officer to decide whether the nature of the data means that the data subject(s) could face any risk, and therefore whether the breach should be notified further (see section 6.1 below).

ii) In a *more complex case* where the amount, or the sensitivity, of the data lost means that the data subject(s)may face a risk to their rights and freedoms, for instance where identity theft might be an outcome of the breach, the Data Protection Officer will determine the level of risk and make a

recommendation to the Executive Director of Corporate Governance on the necessary actions to take, including the need to begin an investigation into the incident and to notify appropriate individuals / bodies (see section 6.1 below). The recommendations will include:

- Whether the breach should be notified to the ICO and the time limit for doing this
- Whether a complex case investigation should be commissioned (see section 7 below)
- Whether it is necessary to inform individuals about the loss and what they should do
- What further actions the University should take to reduce the risk of harm
- Whether any external bodies need to be alerted to the loss e.g. the police, JISC, JANET
- Whether, and what, the third parties whose data has been lost should be told.

# 6.1 Notifying those affected

### *6.1.1 Notifying the ICO*

Where the decision is taken to notify the ICO (which is only likely to be the case in the most complex instances), the following information needs to be provided to that authority by the University's Data Protection Officer, via the ICO's data breach reporting tool:

- A description of the nature of the breach
- The categories of personal data affected
- An approximate number of data subjects affected
- An approximate number of personal data records affected (if different)
- Name and contact details of the Data Protection Officer
- Consequences of the breach whether they have occurred or are likely to occur
- Any measures taken to address the breach
- Any further information relating to the data breach.

This information must be provided to the ICO as soon as possible, and within 72 hours of becoming aware of the breach. If it is not possible to provide all of the information listed above within 72 hours, as much information as possible should be submitted to the ICO as an interim report, along with an explanation of why not all of the detail is available and an estimate of when it will be possible to provide it.

### *6.1.2 Notifying affected individuals*

In the interests of transparency, the University will notify individuals or third parties of any personal data breaches where the University believes there is a risk of harm to the individual's rights and freedoms, for example, where information on a stolen laptop was not encrypted and therefore is clearly accessible to someone who should not have access to it. These notifications should contain the following information at least:

- the name and contact details of the University Data Protection Officer and /or other contact point where more information can be obtained;
- a description of the personal or special category data that is affected by the breach;
- a description of how it is believed the data breach occurred;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects;
- if appropriate, any further actions the data subjects could / should take as a result of the breach to protect their data
- whether the data breach has been reported to the ICO and if not, why not

In cases where only a small number of data subjects are affected, these communications may be sent out by staff members in the department / school / service in which the breach occurred, in order to give a more personalised response.

6.1.3 The Executive Director of Corporate Governance will determine, on the basis of the data lost, who else within the University needs to be made aware of the breach in order to contain and manage the loss. If necessary, a meeting of appropriate staff from relevant University departments will be called to manage the consequences of the breach.

6.1.4 All data security breaches, whether reported to the ICO or not, will be recorded in an internal data breach register held by the Data Protection Officer.

## 6.2 Personal data breaches relating to individuals

6.2.1 Where the data lost relates to individual members of the University community, the Data Protection Officer will make recommendations to the Executive Director of Corporate Governance that determine the extent of the possible harm and consider the actions the University can take to minimise the impact. Examples could include assisting individuals to alert banks, paying for regular credit checks for a given period, alerting any other agencies such as the passport agency.

6.2.2 Where the data lost relates to individuals or organisations for which the University is a data processor, the appropriate member of the Incident Management team (see section 7 below) will alert the Data Protection Officer for the other organisation as soon as possible to notify that organisation of the alleged / actual breach and will offer whatever help is required by the other organisation to help resolve the breach.

# 7. Investigations into personal data breaches

7.1 In the case of a complex personal data breach either occurring or being suspected of occurring, then the top priority will be to start an incident management process. A key part of this process will be an investigation, which will aim to establish the facts about what took place. A properly conducted investigation is vital in helping the University to discover and address the root-cause(s) of the breach in terms of the people, processes or technology involved. Careful investigation of the facts will also support the reporting process that the University is legally or contractually obliged to follow.

7.2 The incident management team (consisting of at least the Chief Information Officer, the Head of Enterprise Platform Services and the Head of Service Delivery from IS, the University Solicitor, a member of UEB and the Data Protection Officer) will decide on the scope of the investigation and lead the process.

7.3 Investigations can be very technically complex, time consuming and may require external expertise. If required, the Chief Operating Officer will commission this expertise.

7.4 Technical explanation about how and when the breach took place, and regular progress updates may be required by the ICO. Summary reports will be referred to the Information Governance group and the Audit and Quality Committee as appropriate.

7.5 If personal data is lost, destroyed or confidentiality is compromised, as a result of a criminal act (e.g. breaking into an office, gaining unauthorised access to a network account, vandalism, cybercrime) then the police must be notified immediately. This will be done by a member of the incident management team via the Action Fraud website https://www.actionfraud.police.uk/ or by calling 0300 123 2040.

7.6 If the data breach includes the loss, theft, damage or compromise of financial information or payment card data, then the head of finance must be informed immediately so that effective action can be taken to minimise financial loss. Financial data is also personal data and is subject to the Payment Card Industry Data Security Standard (PCI DSS)

7.7 Action will be taken by law enforcement bodies against anyone perpetrating a data breach for criminal gain Disciplinary action may be taken by the University against individuals responsible for deliberate or careless data security breaches.

# 8. Learning from data breaches

8.1 Almost all personal data breaches occur as a result of human error. Whenever a personal data breach is suspected, or actually occurs, staff members involved in the breach must consider the cause of the breach and put in place actions to prevent a recurrence. These actions could include (but are not limited to) more vigilance when selecting email addresses, better access controls, multi factor authentication, or putting personal data in an encrypted attachment to an email rather than in the email itself. Staff must also ensure that they have completed the online Information Governance training within the last two years, and refresh that training at least every two years. It is important that lessons are learnt from any data breach and acted upon to prevent any further similar incidents.

# 9. Further Information

For further information on this policy, please contact the University's Data Protection Officer (Samantha.hill@port.ac.uk) or the Information Security Architect (Robbie.walker@port.ac.uk)