# University of Dundee logo

**Data Breaches – What do to next**

**A quick guide for staff**

Staff Guidance on Data Breaches

**Data Breaches**

**WHEN IN DOUBT ABOUT THE MANAGEMENT AND TRANSFER OF PERSONAL OR CONFIDENTIAL DATA, MEMBERS OF THE UNIVERSITY SHOULD ALWAYS SEEK ADVICE FROM INFORMATION GOVERNANCE.**

1. **What is a data breach?**
	1. A personal data breach is defined as “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.” The key is that any breach must concern personal data. While all personal data breaches will be security breaches, not all security breaches will be personal data breaches. This guidance relates to any actual, suspected, threatened or potential personal data breach, including near misses.

* 1. Some examples of personal data breaches are set out in Appendix B.
	2. If a personal data breach is not addressed properly this may, in addition to any

financial, reputational and other losses suffered by the University as an organisation, result in the affected individuals:

* suffering a loss of control over their personal data or limiting their rights in relation to it;
* suffering financial loss;
* suffering a loss of confidentiality or reputation;
* becoming a victim of identity theft or fraud; and/or
* becoming subject to discrimination or some other disadvantage or harm.
1. **What should you do if you think a data breach has occurred?**

### **Notify Information Governance**

2.1 As soon as you become aware of an **actual or suspected** data breach you should inform Information Governance straight away. This can be done by calling the University’s Data Protection Officer on 01382 384082 or by completing the form in Appendix A and sending it to dataprotection@dundee.ac.uk.

The University is under a legal requirement to notify the ICO without undue delay, but not later than 72 hours from when the University first becomes aware of the breach if it is serious.

**It is crucial that you notify Information Governance immediately and provide them with as much information as possible.**

### **Contain the data breach**

2.2 Information Governance will lead any immediate steps to mitigate the data breach, however, they may require your assistance, or the assistance of people in other parts of the University such as DTS, to contain the breach and mitigate its impact.

2.3 Steps to contain the data breach could include:

* isolating or closing a compromised section of the network
* recalling/purging emails
* recovery of released documents
* finding a lost piece of equipment
* changing access codes
* the use of backups to restore lost or damaged data.

2.4 More details on avoiding or mitigating a data breach are available in Appendix C.

**Next steps**

2.5 Information governance will work with you on the next steps. We may need you to contact the person / people who received the information or to contact the person whose data has been released. It is not necessary to contact the data subject in all circumstances.

2.6 If the breach is serious Information Governance will notify the Information Commissioner.

November 2023.

**Appendix A**

**Data Breach Reporting and Evaluation Form**

|  |
| --- |
| **Part A - To be completed and emailed to dataprotection@dundee.ac.uk** |
| **1. ABOUT YOU**  |
| **Name of the organisation** | University of Dundee |
| **Address and contact details**  |  |
| **Name of person who identified breach** |  |
| **2. TIMELINE** |
| **Beginning date of breach**  |  |
| **Date of awareness of breach**  |  |
| **Date of notification by the processor (if applicable)**  |  |
| **Date breach remedied**  |  |
| **3. ABOUT THE BREACH** |
| **Description of the breach** |  |
| **Reason for the breach** |  |
| **Location of breach** |  |
| **What type of data is involved?** Please be specific e.g. names; dates of birth; bank account details; salary details; health details.  |  |
| **How sensitive is the data?** High risk personal data includes special category data (e.g. health data, racial or ethnic origin data, membership of trade union, criminal offences, political or philosophical beliefs, genetic data, biometric data), any information that could be used to commit fraud, information in relation to children or vulnerable adults.  |  |
| **What categories of Data Subject were affected?** E.g. members; beneficiaries; trustees.  |  |
| **How many Data Subjects were affected?**  |  |
| **What has happened to the data?** |  |
| **What are the likely consequences of the breach?** |  |
| **Has any personal data been placed at risk?** |  |
| **Details of the IT systems, equipment, devices, records involved in the breach.** |  |
| **Is the information unique? Will its loss have reputational or legal consequences for the University ?** |  |
| **Is the data bound by any contractual security arrangements?** |  |
| **Part B – To be completed by DPO/Information Governance Team**  |
| **Does the breach require to be notified to the ICO?** If so, please annex the notification to the completed record and any relevant correspondence.Please provide reasoning for your decision in either case.  |  |
| **Does the breach require to be notified to the Data Subjects?** If so, please annex the notification to the completed record and any relevant correspondence.Please provide reasoning for your decision in either event. |  |
| **Do we require to report the incident to the police?** Please provide reasoning for your decision in either event. |  |
| **Do our insurance providers require to be notified?** Please provide reasoning for your decision in either event. |  |
| **Are we required under contract to notify any joint controller or processor?**Please provide reasoning for your decision in either event. |  |
| **5. ABOUT MEASURES IN PLACE BEFORE THE BREACH** |
| **Description of measures in place before the breach**  |  |
| **6. ACTION TAKEN**  |
| **Describe the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.** |  |

**Appendix B**

# Examples of what may be a data breach

# A data breach may include, but is not limited to, the following:

* Human error, for example an email attachment containing personal data being sent to the incorrect recipient or records being deleted accidentally.
* Sharing of passwords or other credentials with third parties.
* Documents being left unattended to be copied, read or photographed by an unauthorised person.
* ‘Blagging’ whereby an individual obtains personal data by deception.
* Unlawful interception of email or telephone communications or online form submissions.
* Loss or theft of a physical file or electronic device containing personal data.
* Loss of a decryption key relating to securely encrypted personal data.
* A Denial of Service (DoS) attack preventing access to personal data for a period of time.
* Damage caused by unforeseen circumstances such as fire or flood.
* Opening or clicking a link within a malicious email which contains malware or viruses.
* A ransomware attack whereby access to systems or records containing personal data is disabled or encrypted.
* A cybersecurity attack whereby personal data are accessed, altered, deleted and/or disclosed by the attacker.

**Appendix C**

**How to avoid and mitigate a data breach**

* University staff members should always use their University-provided email accounts, University devices and approved systems and software when conducting University business.
* Staff should keep personal data safe and make sure that no one has access to it without their authorisation. Some simple security measures could include storing paperwork in a locked cabinet and putting strong passwords on all devices. Additionally, if you deal with sensitive personal information, it is important that you take extra steps to protect it from getting intercepted, lost, damaged or stolen.
* Staff should make sure that no paperwork containing personal information is stored on their desk or in their workspace, including folders, cards and post-it notes. This includes workspace at home.
* Staff should double-check documents before attaching them to an email to ensure the correct document is being attached.
* If you need to send electronic documents, consider encrypting or password-protecting them. This reduces the risk of the wrong person being able to access the documents.
* If you are sending password-protected electronic documents, make sure you send the password separately.
* If you share documents via OneDrive or SharePoint double check you are sharing with the correct person and only that person.
* If people’s email addresses come up automatically when starting a new email message then you have autofill enabled in your settings. While this tool might save time, it could cause a data breach if you send an email to the wrong person by mistake, so it is a good idea to disable it.
* You can set a delay on sending your email to give you time to recall it if you realise you have made an error. More information [here](https://support.microsoft.com/en-us/office/delay-or-schedule-sending-email-messages-026af69f-c287-490a-a72f-6c65793744ba).
* Lastly, familiarise yourself with the ‘How to recall an email’ guidance available on the Microsoft support page: [Recall or replace an email message that you sent - Microsoft Support](https://support.microsoft.com/en-gb/office/recall-or-replace-an-email-message-that-you-sent-35027f88-d655-4554-b4f8-6c0729a723a0).