Report a personal data breach (internal use)

This form is for reporting a personal data breach. The DP & FOI Office will assess whether the breach should be reported to the ICO, and if so, the report will be made by the University’s Data Protection Officer. **Please do not include any of the personal data involved in the breach when completing this form**. For example, do not provide the names of data subjects affected by the breach. If we need this information, we will ask for it later.

You should ensure the information provided is as accurate as possible and supply as much detail as possible.

1. About the breach

**1.1 Please describe what happened:**

**1.2 Please describe how the incident occurred:**

**1.3 How did you discover the breach?**

**1.4 What preventative measures did you have in place?**

**1.5 Was the breach caused by a cyber incident?**

Yes (please complete section 1.14 below)

No

Don’t know

**1.6 When did the breach happen (date/time)?**

* 1. **When did you discover the breach (date/time)?**

**1.8 Categories of personal data included in the breach (tick all that apply):**

Data revealing racial or ethnic origin

Political opinions

Religious or philosophical beliefs

Trade union membership

Sex life data

Sexual orientation data

Gender reassignment data

Health data

Basic personal identifiers (e.g. name, contact details)

Identification data (e.g. usernames, passwords)

Economic and financial data (e.g. credit card numbers, bank details)

Official documents

Location data (e.g. IP addresses, coordinates)

Genetic or biometric data

Criminal convictions and offences data

Other (please provide details)

**1.9 Number of personal data records concerned (e.g. documents, database entries):**

**1.10 How many individuals could be affected?**

**1.11 Categories of individuals affected (tick all that apply):**

Employees

Service users

Subscribers

Students

Customers or prospective customers

Patients

Children

Vulnerable adults

Other (please provide details below)

**1.12 Potential consequences of the breach:**

**1.13 Is the personal data breach likely to result in a high risk to data subjects?**

Yes

No

Not known yet

**1.13.1 Please provide details:**

**1.14 (Cyber incidents only) Recovery time**

We have successfully recovered from the incident with all personal data now at the same state it was shortly prior to the incident

We have determined that we are able to restore all personal data to the same state it was shortly prior to the incident and are in the process of doing this

We are not yet able to determine if personal data can be restored to the same state it was shortly prior to the incident

**1.15 Had the staff member involved in this breach received data protection training in the last two years?**

Yes

No

Don’t know

**1.16 If there has been a delay in reporting the breach, please explain why:**

1. Taking action

**2.1 Describe the actions you have taken, or propose to take, because of the breach:**

**2.2 Have you taken actions to contain the breach? Please describe these remedial actions:**

**2.3 Please outline any steps you are taking to prevent a recurrence, and when you expect they will be completed:**

**2.4 Have you told data subjects about the breach?**

Yes – we have determined that it is likely there is a high risk to the individuals affected and so we have communicated this breach to them

Yes – we have determined that it is unlikely there is a high risk to the individuals affected, however decided to inform them anyway

No – but we are planning to because we have determined it is likely there is a high risk to the individuals affected

No – we determined the incident did not meet the threshold

**2.5 Have you told, or are you planning to tell any other organisation/s about the breach?**

Yes

No

Don’t know

**2.5.1 If you answered yes above, please provide details:**

**Person making this report (name, contact details):**