Imperial College London
Data Breach Plan

Document last updated: March 2025

1 Introduction

1.1 This Data protection breach plan:

1.1.1 places obligations on staff to report actual or suspected breaches of personal data security; and

1.1.2 sets out Imperial's procedure for managing and recording actual or suspected breaches.

1.2 This plan applies to all staff, and to all personal data and sensitive personal data held by the university. This Policy should be read in conjunction with the Data Protection Policy, Information Security Policy and related Codes of Practice.

1.3 For the purpose of this plan:

Data breach team (DBT)	means the team responsible for investigating data incidents whose composition is as set out in Appendix 2.
Data breach	A 'data breach' or 'personal data breach' means a breach of data (due to a failure of one of the data protection legislation principles) leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
Information Commissioner's Office (ICO)	means the UK's independent data protection and information regulator.
Personal data	As defined in Article 4 of the GDPR, Personal Data is; ''personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.
Sensitive / Special Category personal data	As defined in Article 9 of the GDPR, sensitive personal data or special category data is; ''personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.'

2 Responsibility

2.1 The Data Protection Officer (DPO) has overall responsibility for this plan. They, or their representative, are responsible for ensuring it is adhered to by all staff and will oversee the data protection aspects of any incident response.

3 Our duties

3.1 The university processes personal data relating to individuals including staff, students and third parties. As custodians of data, Imperial has a responsibility under the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR or GDPR) including any subsequent replacement or amendment to this legislation, to protect the security of the personal data we hold.

3.2 Imperial must keep personal data secure against loss or misuse. All staff are required to comply with information governance related guidelines and policies (in particular our Data Protection Policy and Information Security Policy) as explained within the Annual Declaration.

4 What can cause a data breach?

A data breach can happen for a number of reasons:

4.1 loss or theft of data or equipment on which data is stored, e.g. loss of a laptop or a paper file;

4.2 inappropriate access controls allowing unauthorised use;

4.3 equipment failure;

4.4 human error, e.g. sending an email to the wrong recipient, not using the BCC function, mail merge error etc;

4.5 unforeseen circumstances such as a fire or flood;

4.6 hacking, phishing and other blagging attacks where information is obtained by deceiving whoever holds it.

5 If you discover a breach

5.1 If you know or suspect a data breach has occurred or may have occurred, you should:

5.1.1 complete a Data Breach Notification Report, which is accessible via Data Breach Notification Report, details of which can be found in Appendix 1.

5.1.2 follow the instructions as set out on - Reporting data breaches

5.2 Where appropriate, you should liaise with your line manager about completion of the report form. However, this may not always be appropriate, e.g. if your line manager is not available or if you have been instructed not to report the incident but you believe that it should be reported. In these circumstances, you should submit the report without consulting your line manager.

5.3 You should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators before initial feedback has been received from the Data Protection Team. The DPO, or member of the Data Protection Team, will acknowledge receipt of the Report Form and take appropriate steps to assist.

6 Managing and recording the breach

6.1 On being notified of a suspected data breach, the DPO will assemble the Data Breach Team based on the specific situation—see Appendix 2.

6.2 The DBT will take immediate steps to establish whether a breach has occurred. If so they will take appropriate action and provide guidance to:

6.2.1 contain the data breach and (in so far as reasonably practicable) recover, rectify or delete the data that has been lost, damaged or disclosed;

6.2.2 assess and record the breach in Imperial's Data Breach Register;

6.2.3 determine whether the university has also breached any duty of confidentiality owed to third parties;

6.2.4 notify appropriate parties of the breach;

6.2.5 take steps to prevent future breaches.

7 Containment and recovery

7.1 The DBT will work with the appropriate people to identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of data.

7.2 The DBT will work with the appropriate people to identify ways to recover, correct or delete data. This may include contacting the police where the breach involves stolen hardware or data.

7.3 Depending on the nature of the breach, the DBT will notify;

7.3.1 the University's cyber liability insurer; and/or.

7.3.2 the University's professional indemnity insurer.

7.4 The DBT will consider whether to obtain external security breach support via the cyber security insurer's breach vendor panel (aka breach response panel). The most recent version of the cyber liability insurance policy and endorsements to it should be checked for up-to-date details of the composition of the breach response panel.

8 Assess and record the breach

8.1 Having dealt with containment and recovery (see paragraph 0), the DBT will assess the risks associated with the breach in line with the Data Breach Matrix (see Appendix 3), including to consider the following;

- 8.1.1 what type of data is involved?
- 8.1.2 how sensitive is the data?
- 8.1.3 who is affected by the breach, i.e. the categories and approximate number of data subjects involved;
- 8.1.4 the likely consequences of the breach on affected data subjects, e.g. what harm can come to those individuals, are there risks to physical safety or reputation, identity theft or financial loss?
- 8.1.5 where data has been lost or stolen whether there are any protections in place such as encryption?
- 8.1.6 what has happened to the data, e.g. if data has been stolen, could it be used for harmful purposes?
- 8.1.7 what could the data tell a third party about the data subject, e.g. the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people?
- 8.1.8 what are the likely consequences of the personal data breach, e.g. loss of reputation, loss of business, liability for fines?
- 8.1.9 are there wider consequences to consider, e.g. loss of public confidence in an important service we provide?

8.2 This information will be recorded in the Data Breach Register which the Data Protection Officer oversees.

9 Notifying appropriate parties of the breach

9.1 The DBT will consider whether to notify:

- 9.1.1 affected data subjects;
- 9.1.2 the police;
- 9.1.3 the ICO;
- 9.1.4 any other parties, e.g. insurers, external breach support providers
- 9.1.5 partner organisations where their data is affected or as part of a required process. Partners would include (but not limited to) the NHS, NHS Digital, commercial partners, government agencies such as the Department for Education or the Department for Health and Social Care and organisations as required under the Data Security and Protection Toolkit (DSPT) protocol.

9.2 Notifying the ICO:

The University is required to report all data breaches (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals) to the ICO within 72 hours. If the DBT is unsure whether or not to report, the presumption should be to report. The DBT will take account of any relevant ICO guidance and requirements set by the ICO. The notification must include at least:

- a description of the data breach, including the numbers of data subjects affected and the categories of data affected;
- the name and contact details of the DPO (or other relevant point of contact);
- the likely consequences of the data breach; and
- any measures taken by the controller to remedy or mitigate the breach.

9.3 Notifying data subjects:

In the event of a data breach causing 'high risk' to data subjects, the controller (which is most cases will be the University) must notify the affected data subjects without undue delay.

9.4 The notification must include at least:

- the name and contact details of the DPO (or other relevant point of contact);

- the likely consequences of the data breach; and
- any measures taken by the controller to remedy or mitigate the breach.

However, the controller may be exempt from this requirement if:

- the risk of harm is remote because the affected data are protected (e.g., through strong encryption, mitigations etc.);
- the controller has taken measures to protect against the harm (e.g., suspending affected accounts); or
- the notification requires disproportionate effort (in which case the controller must issue a public notice of the breach).

In determining whether to notify affected data subjects, the DBT will have regard to the above requirements and any applicable ICO guidance.

9.5 Notifying the police:

The DBT will already have considered whether to contact the police for the purpose of containment and recovery (see paragraph 7). Regardless of this, if it subsequently transpires that the breach arose from a criminal act perpetrated against, or by a representative of, the University, the DBT will notify the police and/or relevant law enforcement authorities.

9.6 Notifying other parties

9.6.1 If the breach has been notified to any or all of the parties listed at paragraphs 9.1.1 through 9.1.3, the cyber liability insurers should be notified too.

9.6.2 Notification to the cyber liability insurers should take place as soon as possible in accordance with the section entitled “Notice of claim or circumstance that might lead to a claim” in the cyber liability insurance policy. Please check the most recent version of the policy and the endorsements to it for the most up-to-date outline of the notification requirements.

9.6.3 The cyber liability insurers must be provided with all assistance and co-operation and relevant documentation concerning the breach as soon as is possible.

9.6.4 Post-notification, if the University receives any demands, claims or summons, it must provide copies of these to the cyber liability insurers.

9.6.5 The University is also contractually obliged to comply with any request from the cyber liability insurers to notify the police or other law enforcement agencies.

9.6.6 The DBT will consider whether there are any legal or contractual requirements to notify any other parties.

10 Preventing future breaches

The DBT will:

- establish what security measures were in place when the breach occurred;
- assess whether technical or organisational measures could be implemented to prevent th e breach happening again;
- consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- consider whether it is necessary to conduct a risk assessment or review / update a Data Protection Impact Assessment (if one exists);
- debrief DBT members following the investigation;
- where additional oversight / actions are required, the Data Protection Officer will bring the incident for the awareness of Imperial’s Senior Information Risk Owner and any/all university leadership personnel.

11 Monitoring and review

- We will monitor the effectiveness of all our policies and procedures regularly and conduct a review and/or update as appropriate.
- Our monitoring and review exercises will include looking at how our policies, code of practice and procedures are working in practice to reduce the risks posed to the University.

12 Staff awareness and training

12.1 Key to the success of our systems is staff awareness and understanding.

12.2 We provide training to staff:

- at induction;
- refresher training.

12.3 We update senior management:

- when there is any change to the law, regulation or our policy;
- where significant new threats are identified;
- in the event of an incident affecting the university or another HEI institution.

13 Reporting concerns

13.1 Prevention is always better than cure.

13.2 Data security concerns may arise at any time.

13.3 We encourage you to report any concerns you have to the DPO. This helps us capture risks as they emerge, protect the university from data breaches, plus keep our processes up-to-date and effective.

14 Consequences of non-compliance

14.1 Failure to comply with this plan and associate policies (e.g. Data Protection or Information Security) puts you and the university at risk.

14.2 Failure to notify the DPO of an actual or suspected data breach is a very serious issue.

14.3 You may be liable to disciplinary action if you fail to comply with the provisions of this, and all related plans, policies and procedures.

APPENDIX 1
Notification of Data Breach

The following details are collected via the online notification form.

1.Reporting party first name
2.Reporting party surname
3.Reporting party email address (we will use this to contact you)
4.Please choose from the following list the area of College affected
• Advancement • Business School • Faculty of Engineering • Faculty of Medicine • Faculty of Natural Sciences • Support Services • Other
5.Telephone number (optional)
Please state the department affected
7.Date breach occurred (if known)
Please input date (DD/MM/YYYY)
8.Date breach discovered
Please input date (DD/MM/YYYY)
9.Did the incident result in data being exposed internally, externally or both?
• Internally • Externally • Both
10.Please describe the incident, what has occurred and how.
11.Cause of breach please see guidance available on College website (https://www.imperial.ac.uk/admin-services/secretariat/information-governance/data-protection/processing-personal-data/)
• Data emailed to incorrect recipient • Failure to bcc • Data posted to incorrect recipient • Phishing/Quishing/Smishing/Vishing • Unauthorised access • Loss/theft of paperwork • Ransomware • Failure to redact • Verbal disclosure • Hardware / software misconfiguration • Malware • Incorrect alteration • Incorrect destruction • Denial of access to data • Other

12.DART entry if known (Data Asset Registration Tool - DART)
13.Data type put at risk please see guidance available on College website (Data Protection Guidance)
• Personal data • Special category data • Criminal conviction data • Other
14.Number of individuals (data subjects) affected
• 1-9 • 10-99 • 100-1k • 1k-10k • 10k-100k • 100k and above • unknown
15.Are the individuals (data subjects) aware?
• Yes • No • Unknown
16.Actions taken so far?
17.What measures (if any) were in place to prevent this incident occurring? What are the potential consequences (if any) for the person(s) affected by the breach?
18.Who else have you notified about the incident?

APPENDIX 2

Data Breach Responsibility and Oversight

College staff who have specific responsibility for receiving data breach or information security incident reports are:

Initial Breach Notification – Data Breach Team

- Data Protection Officer
- Deputy Data Protection Officer
- Chief Information Security Officer
- Information Compliance Manager – Access and Records
- Head of ICT Governance and Compliance
- Information and Compliance Officer

Breach response (where appropriate)

- Director of Institutional Compliance and Risk Management
- ICT Cyber Office
- Faculty IG / DP Leads
- Data Protection Coordinators
- Information Asset Owner for the data breached
- Any other person whom any of the above consider appropriate to consult with

Where ICO notification required

- University Secretary
- Deputy University Secretary and General Counsel - Senior Information Risk Owner (SIRO)

APPENDIX 3

Data Breach Matrix

1. **Introduction**
   - 1.1 To be read in coordination with the ICL Data Breach Plan which outlines initial response to a data incident and based on the 'enisa - Recommendations for a methodology of the assessment of severity of personal data breaches'.
   - 1.2 Once a data incident has been identified as a breach and following initial investigation, risk mitigation and breach containment the next step of the investigation relates to whether of not the breach meets the threshold for notification to the UK Data Protection Regulator and / or the affected data subjects.
   - 1.3 To require notification to the Information Commissioners Office, the UK GDPR states the breach must represent a 'Risk' to the rights and freedoms of natural persons (Article 33[1]).
   - 1.4 To require notification to the data subjects involved, the UK GDPR states the breach must represent a 'High Risk' to the rights and freedoms of natural persons (Article 34[2]).
   - 1.5 To assist in identifying whether a 'Risk' and/or 'High Risk' has occurred the Data Protection Team will balance each data breach reported in accordance with the following 3 step process;
2. **Step 1 – Data Processing Context (DPC)**
   - 2.1 Step 1 consists of assigning a DPC Score between 1 and 4 based on the context of the incident occurred;
     - 2.1.1 **1 point** - Where the breach involves simple data and the controller is not aware of any aggravating factors.
     - 2.1.2 **2 point** - When the volume of data and/or the characteristics of the controller are such that certain profiling of the individual can be enabled or assumptions about the individual's social/financial status can be made.
     - 2.1.3 **3 point** - When the data and/or the characteristics of the controller can lead to assumptions about the individual's health status, sexual preferences, political or religious beliefs.
     - 2.1.4 **4 point** - When due to certain characteristics of the individual (e.g. vulnerable groups, minors), the information can be critical for their personal safety or physical/psychological conditions.
3. **Step 2 – Ease of Identification (EI)**
   - 3.1 Step 2 consists of assigning an EI Score between 1 and 4 based on the apparent ease of identification which the breached data represents for the data subjects involved;
     - 3.1.1**1 point** - Negligible (very hard to identify individuals).
     - 3.1.2 **2 point** - Limited (some effort needed for identification).
     - 3.1.3 **3 point** - Significant (identification fairly straightforward).
     - 3.1.4 **4 point** - Maximum (direct and easy identification).
4. **Step 3 – Circumstances of the Breach (CB)**
   - 4.1 Step 3 balances, assigns and adds up scores based on the circumstances of the breach;
     - 4.1.1Confidentiality
       - 4.1.1.1 **0 point** - No unauthorised (illegal) access
       - 4.1.1.2 **0.25 point** - Leak to known recipients
       - 4.1.1.3 **0.5 point** - Leak to unknown recipients
     - 4.1.2 Integrity
       - 4.1.2.1 **0 point** – No alteration of data
       - 4.1.2.2 **0.25 point** – Alteration of data, recoverable
       - 4.1.2.3 **0.5 point** – Alteration of data, not recoverable
     - 4.1.3 Availability

[1] https://www.legislation.gov.uk/eur/2016/679/article/33
[2] https://www.legislation.gov.uk/eur/2016/679/article/34

4.1.3.1 **0 point** – no loss of data.
4.1.3.2 **0.25 point** – Loss of data, temporal issues
4.1.3.3 **0.5 point** – Loss of data, no recovery

4.1.4 Malicious Intent

4.1.4.1 **0 point** – No malicious intent
4.1.4.2 **0.5 point** – Malicious intent

5. The Final Score

5.1 Once you have collated the above data points the following calculation can be made;

$$(DPC \times EI) + CB$$

<2: Low Severity

>=2: Medium Severity

>=3: High Severity (to report to ICO)

>=4: Very High Severity (to report to ICO and Data Subjects)