Imperial College Union
Data Breach Plan

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 the Union'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 Union. This Policy should be read in conjunction with the College's Data Protection Policy, Imperial College London Information Security Policy and related Codes of Practice. These provide more detailed guidance on the correct handling of personal data.

1.3. For the purpose of this plan:

Data breach team means the team responsible for investigating data security breaches whose composition is as set out in Appendix 2.

Data security breach means any act or omission that may compromise the security of personal data, e.g. accidental loss, destruction, theft, corruption or unauthorised disclosure of personal data.

Information Commissioner's Office (ICO) means the UK's independent data protection and information regulator.

Personal data means information relating to identifiable individuals such as students, contractors, alumni, former employees, job applicants, agency, contract and other staff, suppliers and marketing contacts. This includes expression of opinion about the individual and any indication of someone else's intentions towards the individual. Personal data includes 'sensitive personal data'.

Sensitive personal data means personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings.

2. **Responsibility**

2.1. The Managing Director (MD) has overall responsibility for this plan. They are responsible for ensuring it is adhered to by all staff.

3. **Our duties**

3.1. The Union processes personal data relating to individuals including staff, students and third parties. As custodians of data, the Union has a responsibility under the Data Protection Act 1998 (DPA 1998), including any subsequent replacement or amendment to this legislation, to protect the security of the personal data we hold.

3.2. The Union must keep personal data secure against loss or misuse. All staff are required to comply with information security guidelines and policies (in particular our Data Protection Policy and Information Security Policy).

4. **What can cause a data security breach?**

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;
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 security breach has occurred or may occur, you should:
5.1.1. complete a Notification of Data Security Breach at https://www.imperialcollegeunion.org/data-breach (the template for which can be found in Appendix 1 below as well as at https://www.imperialcollegeunion.org/sites/default/files/Notification-of-data-security-breach-union.docx)

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 directly 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. The Data Breach team will acknowledge receipt of the report form and take appropriate steps to deal with the report in collaboration with the data breach team.

5.4. All staff should be aware that any breach of the DPA 1998 or the General Data Protection Regulation (GDPR) may result in disciplinary action being taken under the College's Disciplinary Procedures.

6. Managing and recording the breach

6.1. On being notified of a suspected data security breach, a Senior Manager or Systems Manager will assemble the data breach team—see Appendix 2. The data breach team will be led by the Systems Manager or a designated Senior Manager.

6.2. The data breach team will take immediate steps to establish whether a breach has, in fact, occurred. If so, the data breach team will take appropriate action to:
6.2.1. contain the data breach and (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 the Union's Data security breach register;
6.2.3. determine whether the Union has also breached any duty of confidentiality owed to third parties by the Union;
6.2.4. notify appropriate parties of the breach;
6.2.5. take steps to prevent future breaches.

These are explained in the sections below.

7. Containment and recovery

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

7.2. The data breach team will work with the appropriate people in the Union and College to identify ways to recover, correct or delete data. This may include contacting the police, e.g. where the breach involves stolen hardware or data.

7.3. Depending on the nature of the breach, the data breach team will notify the College's professional indemnity insurer.

8. Assess and record the breach

8.1. Having dealt with containment and recovery (see paragraph 7), the data breach team will assess the risks associated with the breach, including:

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 for the College, 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 should be recorded in the College's Data breach register.

9. Notifying appropriate parties of the breach

9.1. The data breach team 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 or commercial partners.

9.2. Notifying data subjects

In determining whether to notify affected data subjects, the data breach team will have regard to ICO guidance that notification should have a clear purpose, e.g. to warn individuals to take protective action. The data breach team will consider who should be notified, how and what they should be told, taking into account the following factors:

9.2.1. can notification help the individual(s), e.g. could individuals act on the information to mitigate risks by cancelling a credit card or changing a password?

9.2.2. will notification mitigate the harm done to an individual or pointlessly alarm them in circumstances where they can do nothing with that information?
9.2.3. are there any legal or contractual requirements to notify the data subject, e.g. in our staff or student terms and conditions?
9.2.4. is there a danger of over notifying—not every incident will warrant notification;
9.2.5. what is the best way of notifying affected individuals—taking into account the security of the notification method and the urgency of the situation?
9.2.6. do any individuals or categories of individuals need to be treated with special care, e.g. if the breach involves data relating to children or vulnerable adults?
9.2.7. what information should be provided to individuals about the steps they can take to protect themselves and what we can do to help them?
9.2.8. how should affected individuals contact us for further information or to ask questions—this could be a helpline number or a web page?
9.2.9. will notification help the College meet its security obligations?

9.3. Notifying the police

The data breach team 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 College, the data breach team will notify the police and/or relevant law enforcement authorities.

9.4. Notifying the ICO

Unless the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals, the data breach team will notify the ICO within 72 hours when a breach has occurred. If the data breach team is unsure whether or not to report, the presumption should be to report. The data breach team will take account of relevant ICO guidance, summarised below:

The potential harm to data subjects

This is the overriding consideration in deciding whether a breach of data security should be reported to the ICO. Detriment includes emotional distress as well as both physical and financial damage. It can include:

- exposure to identity theft through the release of non-public identifiers, e.g. passport number
- information about the private aspects of a person's life becoming known to others, e.g. financial circumstances

Significant actual or potential detriment should be reported, whether because of the volume of data, its sensitivity or a combination of the two.

There is no need to report where there is little risk that individuals would suffer significant detriment, e.g. because a stolen laptop is properly encrypted or the information is publicly-available information.

The volume of personal data

There should be a presumption to report to the ICO where:

- a large volume of personal data is concerned, and
- there is a real risk of individuals suffering some harm

It will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high, e.g. because of the circumstances of the loss or the extent of information about each individual.

The ICO provides two examples:

- loss of an unencrypted laptop holding names, addresses, dates of birth and National Insurance numbers of 100 individuals would be reportable
- loss of a marketing list of 100 names and addresses (or other contact details) where there is no particular sensitivity of the service being marketed would not be reportable

The sensitivity of data

There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress.

This is most likely to be the case where the breach involves sensitive personal data. If the information is particularly sensitive, even a single record could trigger a report.

The ICO provides two examples:

- theft of a manual paper-based filing system (or unencrypted digital media) holding the personal data and financial records of 50 named individuals would be reportable
- breach of a similar system holding the trade union subscription records of the same number of individuals (where there are no special circumstances surrounding the loss) would not be reportable

9.5. Notifying other parties

The data breach team will consider whether there are any legal or contractual requirements to notify any other parties.

10. Preventing future breaches

The data breach team will:

10.1. establish what security measures were in place when the breach occurred;
10.2. assess whether technical or organisational measures could be implemented to prevent the breach happening again;
10.3. consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
10.4. consider whether it is necessary to conduct a privacy risk assessment or update an existing privacy risk assessment;

10.5. debrief data breach team members following the investigation.

11. Monitoring and review

11.1. We will monitor the effectiveness of all our policies and procedures regularly, and conduct a full review and update as appropriate, at least annually.

11.2. Our monitoring and review exercises will include looking at how our policies and procedures are working in practice to reduce the risks posed to our firm.

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:

12.2.1. at induction;

12.2.2. refresher training as appropriate.

12.3. We update senior management:

12.3.1. when there is any change to the law, regulation or our policy;

12.3.2. where significant new threats are identified;

12.3.3. in the event of an incident affecting the College or another HEI institution.

13. Reporting concerns

Prevention is always better than cure. Data security concerns may arise at any time. We encourage you to report any concerns you have to Union Systems Manager or Head of Finance and Resources. This helps us capture risks as they emerge, protect the Union from data security breaches, and 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, the Union and the College at risk. Failure to notify the Breach Team of an actual or suspected data security breach is a very serious issue.

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

Document last updated: June 2018

APPENDIX 1

Notification of Data Security Breach

Please act promptly to report any data breaches. If you discover a data breach, please notify the Union by calling reception immediately on 020 7594 8060 (hours 9am-5pm), complete this form and email it to 365-uniondataprotection@groups.imperial.ac.uk.

We will need to contact you as part of our investigation, so please ensure you provide your contact details. If the data breach concerns your team or department, you and your colleagues may also be asked to assist with notifying affected individuals (where that is necessary) and to help prepare a notification to the Information Commissioner (where notification is required).

Name and contact details of person reporting incident (email address, telephone number):	
Date incident was discovered:	
Date(s) of incident:	
Place of incident (this could be a College campus, or an external location):	
How did the incident happen/ a brief description of the incident:	
What personal data has been placed at risk? Also, please specify if any financial or sensitive personal data has been affected and provide details of the extent.	
How many individuals have been affected?	
Are the affected individuals (or any one of them) aware that the incident has occurred?	
Are you aware if any affected individuals have complained to the College or to any external party about the incident?	
On the basis of what you know, what are the potential consequences and adverse effects on the affected individuals?	
Brief description of any action taken at the time of discovery of the incident (e.g. has any mitigation action been taken, has any lost data been recovered):	

To your knowledge, what measures were in place to prevent an incident of this nature occurring?	
Please provide copies or extracts of any local (e.g. team, departmental or Faculty) policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.	
Who else have you notified about this incident?	
Is there anything else you would like to draw to our attention in relation to this incident?	

APPENDIX 2

Data Breach Team Assembly and Responsibility

Union staff who have specific responsibility for receiving data breach or information security incident reports and for initiating investigations are:

☐ Managing Director

☐ Head of Finance and Resources

☐ Head of Student Voice

☐ Union President

☐ Other Senior Managers

☐ Systems Manager

☐ Any other person whom any of the above consider appropriate to consult with