Imperial College London
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 College'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 College. This Policy should be read in conjunction with the College's Data Protection Policy, 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	A 'data security breach' or 'personal data breach' means 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;
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 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

The Data Protection Officer (DPO) has overall responsibility for this plan. They are responsible for ensuring it is adhered to by all staff.

3 Our duties

3.1 The College processes personal data relating to individuals including staff, students and third parties. As custodians of data, the College 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 The College 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?

A data security 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 or fax 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 (the template for which can be found in Appendix 1 below as well as on https://www.imperial.ac.uk/admin-services/secretariat/information-governance/data-protection/

5.1.2 email the completed form to (365-dataprotectionoffice@groups.imperial.ac.uk) as per the instructions as set out on http://www.imperial.ac..uk/admin-services/legal-services-office/data-protection/

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 direct to the DPO 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 DPO 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 2018, the General Data Protection Regulation (GDPR) or other data protection legislation 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, the DPO will assemble the data breach team—see Appendix 2. The data breach team will be led by the DPO.

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 College's Data security breach register;

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

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 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 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;

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

7.3.2 the College's professional indemnity insurer.

7.4 The data breach team 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 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 will be recorded in the College's Data breach register. The College is obliged to keep records of all data breaches, comprising the facts and effects of the breach and any remedial action taken.

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, 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 College 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 data breach team is unsure whether or not to report, the presumption should be to report. The data breach team will take account of any relevant ICO guidance. 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 College) must notify
the affected data subjects without undue delay. 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);
- 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 data breach team will have regard to the above requirements and any applicable ICO guidance.

9.4 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.

9.5 Notifying other parties

9.5.1 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.

9.5.2 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.

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

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

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

9.5.6 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:

- establish what security measures were in place when the breach occurred;
- assess whether technical or organisational measures could be implemented to prevent the 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 privacy risk assessment or update an existing privacy risk assessment;
- debrief data breach team members following the investigation.

11 Monitoring and review

- We will monitor the effectiveness of all our policies and procedures regularly, and conduct a full review and update as appropriate, at least annually.
- 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. 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 the DPO. This helps us capture risks as they emerge, protect the College from data security breaches, and keep our processes up-to-date and effective.

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 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 the DPO. This helps us capture risk as they emerge, protect the College 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 and the College at risk. Failure to notify the DPO 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.

APPENDIX 1
Notification of Data Security Breach

Please act promptly to report any data breaches. If you discover a data breach, please notify your Head of Department or Head of Division immediately, complete this form and email it to 365-dataprotectionoffice@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

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

- Head of Central Secretariat
- Head of Legal Services
- Data Protection Officer
- Legal Services Officer
- Head of Information Governance
- Network & Security Services Manager
- Faculty IG / DP Leads
- Any other person whom any of the above consider appropriate to consult with
- Relevant security officers