1. POLICY STATEMENT

1.1 Imperial College needs to collect, store and process personal data in order to carry out our functions and activities. The College is a registered Data Controller and is committed to full compliance with the Data Protection Act 1998 to ensure the protection and correct management of personal data, regardless of the medium in which it is held.

1.2 All College staff, students and other authorised third parties, who have access to any personal data held by or on behalf of the College, must adhere to the College’s Data Protection Policy and associated Codes of Practice.

1.3 This Policy should be read in conjunction with the College’s Information Security Policy and related Codes of Practice. These provide more detailed guidance on the correct handling of personal data.

2. PROCESSING PERSONAL DATA

2.1 Personal data is information that relates to a living individual directly or indirectly, from which they can be identified. It includes factual information or expressions of opinion about the individual. The individual is known as the ‘data subject’. The College, and therefore its staff, students and authorised third parties must comply with eight principles set out in the Act when personal data is processed. Processing includes any activity that involves the handling of personal data including its collection, use, storage, adaptation, dissemination or disposal. The principles provide that personal data must be:

(1) Processed fairly and lawfully, and shall not be processed unless certain conditions are met
(2) Processed for limited purposes and in an appropriate way.
(3) Adequate, relevant and not excessive for the purpose.
(4) Accurate and, where necessary, kept up to date.
(5) Not retained longer than necessary.
(6) Processed in line with the rights of the data subject.
(7) Kept securely and protected from unauthorised access or accidental loss.
(8) Not transferred outside the European Economic Area unless there is an adequate level of protection for the rights of data subjects in relation to the processing of personal data.

3. CONDITIONS OF PROCESSING

3.1 The Act sets out conditions for processing personal data. Usually the College will only process data when the data subject has consented to the processing. Students agree to the processing of their personal data on registration with the College. Staff are informed that the College processes personal data in the Core Terms and Conditions of Service.

3.2 In other circumstances it will be assumed that consent has been given by the data subject for their personal data to be used for the purposes advised at the point of collection of that data. Where the data is defined as sensitive personal data under the Act, explicit consent must be obtained from the data subject before processing can proceed. The Act defines sensitive personal
3.3 Where there is a legal obligation to process data without seeking the consent of the data subject(s), a record will be kept of the circumstances and justification used.

4. DATA SECURITY

4.1 Personal data, whether held electronically or in paper form, must be kept securely at all times. College staff, students and authorised third parties should ensure that appropriate technical and organisational measures are in place to prevent unauthorised access or accidental disclosure or loss when data is being stored or transferred. Data security measures are set out in the College’s Information Security Policy. Technical measures, for example, include using encryption tools to protect personal data held in electronic form. Organisational measures, for example, include storing paper records containing personal data in locked cabinets or rooms.

4.2 It is essential that if personal data is lost, compromised, misdirected or stolen, that it is reported as an information security incident. If the way in which data is handled puts it at risk then this should be similarly reported to the Central Secretariat or Legal Services Office.

4.3 Personal information should not be disclosed orally or in writing to unauthorised third parties without the consent of the data subject.

5. RETENTION OF PERSONAL DATA

5.1 Personal data, irrespective of the medium, shall not be kept for longer than is necessary for the purpose or purposes for which it was obtained, or as required to comply with other legislation. Some personal data will be permanently retained where it has designated archival status.

5.2 The College will maintain a Retention Schedule to provide guidance on the length of time records should be retained before they should be securely destroyed or transferred to the College Archives. The College’s Retention Schedule is available at https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/records-and-archives/public/Retention-Schedule-version-2010.pdf

6. RIGHTS OF ACCESS TO PERSONAL DATA

6.1 The College respects the rights of individuals to access the personal data that is being held about them; to check that it has been fairly obtained and accurate, and to have such data corrected or deleted where appropriate. The College also recognises the rights of individuals to prevent their personal data being processed for direct marketing or to object to the processing of personal data where such processing could cause them significant damage or
distress.

7. RESPONSIBILITIES

7.1 Staff, students and authorised third parties
All College staff, students and authorised third parties must adhere to the College’s Data Protection Policy and associated Codes of Practice when processing personal data, whether held in paper form or electronically. Compliance with the policy forms part of the Core Terms and Conditions of Service for College staff and forms part of the Regulations for Students. Non-compliance with this policy could lead to disciplinary action being taken. Any actual, or suspected, data security breaches (such as accidental exposure or loss, or unauthorised access) must be reported to the Central Secretariat or Legal Services Office without delay.

7.1.1 All staff and students are responsible for ensuring the personal data they provide to the College is accurate and up to date.

7.2 Heads of Departments and Heads of Divisions
Heads of Departments and Heads of Divisions are responsible for ensuring that staff, students and other authorised individuals within their department or division are aware of, and comply with the College’s Data Protection policy and Codes of Practice.

7.3 College Data Protection Officer
The College Data Protection Officer is required to maintain the College’s notification of its processing of personal information with the Information Commissioner’s Office. They will handle the processing of personal data requests and will provide advice and training to members of the College in relation to data protection.

7.4 Information and Communication Technologies Security Team
The ICT Security team are responsible for carrying out day-to-day activities related to Information Security as required to protect the College and its information assets and assisting the Information Governance Unit and the Central Secretariat to build and update Information Security Policy and related Codes of Practice.

7.5 Head of Information Governance
The Head of Information Governance reports to the Chief Information Officer and is responsible for keeping College’s Information Security Policy up-to-date in association with the Central Secretariat.

7.6 Archives and Corporate Records Management Unit
The Archives and Corporate Records Management Unit are responsible for maintaining the College’s Retention Schedule.

7.7 Departmental Data Protection Co-ordinators
The Departmental Data Protection Co-ordinators are required to provide advice to staff and students within their departments or divisions on the implementation of, and compliance with this policy and on the observance of the associated Codes of Practice.
7.8 Data processors
Contracts with third party data processors will include the contractual responsibility that any processing of personal data carried out on behalf of the College is done in compliance with the College’s Data Protection Policy and the requirements of the Act.
# Version History

<table>
<thead>
<tr>
<th>Version/Status</th>
<th>Release Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0/Approved</td>
<td>January 2013</td>
<td>Approved</td>
</tr>
<tr>
<td>1.1/Revised – In Review</td>
<td>February-June 2016</td>
<td>Fully revised version by Jessica Silver, College Data Protection Officer and John Hancock, Head of Central Secretariat. Reviewed by John Neilson, College Secretary and Mike Russell, CIO</td>
</tr>
<tr>
<td>1.2/In Review</td>
<td>July 2016</td>
<td>Reviewed by IGSG.</td>
</tr>
</tbody>
</table>