Imperial College
London

Imperial College

Data Privacy Impact Assessment

Doc. Ref.	: Data Privacy Impact Assessment
Version	: 2.0
Status	: Approved
Date	: 01/05/2018
Approved by	: John Neilson, College Secretary
Review by	: 01/05/2019

1. INTRODUCTION

1.1 This Code of Practice is to be read in conjunction with the Information Security Policy, Data Protection Policy and wider Information Governance Policy Framework.

1.2 It governs the completion of the Data Privacy Impact Assessment, whether it be on an 'as required' basis (within ICT project management methodology or wider business as usual application), or for Information Asset Owners to complete as part of their annual review of their information assets.

2. DATA PRIVACY IMPACT ASSESSMENT

2.1 Information Asset Owners are required to manage their information assets in accordance with the responsibilities outlined in the Information Governance Policy Framework.

2.2 Information Asset Owners should be prepared to undertake a review at the very least annually, and certainly when there is a significant change in the asset, the hosting of the asset, or significant legislative or policy changes which impact on the personal data held within.

2.3 Information Asset Owners must ensure that the security of their asset meets the requirements of the College's Information Security Policy, such that:

- All users are properly authorised before they may access the information.
- Appropriate levels of security are adopted according to the value and/or sensitivity of the information.
- They must report any incident which results in, or has the potential to result in, a breach of security to the ICT's Service Desk immediately. Concerned individuals may contact any senior members of ICT or College directly. (Refer to these locations for contact details: http://www.imperial.ac.uk/admin-services/ict/about-ict/leadership-organisational-structure/ and http://www.imperial.ac.uk/admin-services/secretariat/information-for-staff/college-contact-lists/principal-officers-and-their-assistants/)
- They must carry out a Data Privacy Impact Assessment of their assets as part of the annual information asset register review.

2.3.1 Every Information Asset Owner agrees to take at all times every reasonable care to ensure that all material held on information assets they own:

- are lawful.
- comply with Section 11 "Conditions of Use of IT Resources (Acceptable Use Policy)" in the College's Information Security Policy.
- do not contain links to unlawful material or material that does not comply with the College Conditions of Use of (IT) Facilities.
- do not, purport to promote or comment, in the College's name, upon any commercial goods, products or services, unless approved by a head of Department.

- do not purport to promote or comment upon any company, partnership, consortium or consultancy or any "private" activity of the Information Asset Owner or any other person, unless approved by a Head of Department.

2.3.2 Any individually owned information on College information assets:

- Should not display coat-of-arms, crest, logo, logotype, page layout or format belonging to Imperial College.
- The material must be relevant to or associated with the information owner's authorisation to use College IT facilities.
- These regulations and the appearance of individually owned information, howsoever referenced, do not imply in any way whatsoever that the College approves or endorses individually owned information or takes any responsibility for individually owned information itself or any material or opinions contained therein.

An approved disclaimer must appear on all individually owned information indicating that this information is not formally published by the College.

2.4 All staff at Imperial are responsible for following good information security practice to ensure information held by the College is properly protected, irrespective of the format in which it is held. Heads of Departments (HoDs) are expected to have oversight of the information security practice in their department, as part of their management responsibilities. As part of this process, HoDs are required to review assets within their department, and ensure that the College's Information Asset Register represents an accurate picture of all managed assets.

2.5 The asset register also allows ICT Security and IT Governance to identify specific information assets where departments may benefit from specialised ICT support, and to plan information security audits. Although the information asset register is managed by ICT, consideration should also be given to the security of paper records.

2.6 Information assets are to be identified as logical collections. That is, information collected for a research study could be held in various media including a number of laptops, a group space drive and USB sticks. This should be recorded as one entry describing each medium and how they are kept secure.

2.7 Departments must declare any information assets held by the department. Please list any additional systems purchased locally for digital/records storage, as 'departmental system' assets. Departments should contact ICT Security via the ICT Service Desk if they require advice in declaring additional information assets. Examples of such assets include cloud storage systems and paper filing systems.

2.8 When reviewing the information assets for their department, HoDs should consider:

- Any new information assets that need to be added to the register
- Any information assets that are no longer in use and can be removed from the register

- Any information assets where use has changed, where the asset register needs to be updated
- Any policy changes that affect the way information assets are used by the department

2.9 It is recognised that HoDs (or their delegate) will not have comprehensive knowledge of all the information which staff in their department are working with, or all the ways this information is stored. Departments are encouraged to reflect broadly on the key risks associated with information the department holds, and where this information is stored, when completing the information asset register. Departments may find it helpful to focus on the transmission of data, especially where data is sensitive or transmitted outside of the College. Please contact ICT Security via the ICT Service Desk for further guidance.

APPENDIX A: STRUCTURE OF INFORMATION ASSET REGISTER

Field	Explanation
Information Asset Owner	Who is responsible for the information stored in this information asset, and is the point of contact for queries about this information asset?
Information Asset Administrator	The role of the information asset administrator is defined in the College's Information Governance Policy Framework document and can be summarised as the most senior day-to-day user of the asset.
Name of the Information Asset	A unique name for the information asset
Description of the Information Asset	Please provide a brief description of the information asset. Where possible, please provide a brief overview of the kinds of information held.
Status	IAR field only – Temporary, Approved or Inactive
Classification	• *Does the asset contain sensitive data? What are the risks associated with this data and how are they mitigated?* Sensitive data includes: o Commercially sensitive administration or research data o Sensitive personal data, as defined in the Data Protection Act. This encompasses information related to an individual's racial or ethnic origin, religious beliefs, physical or mental health or condition, sexual life, political opinions, trade union membership, or criminal convictions or proceedings. o Personal financial data o Patient Identifiable Data held for research purposes o Data relating to sensitive areas of research Personal data, not included in the categories above, but where accidental

	release of the data is likely to be detrimental or distressing to the individuals the data is about.
Media Type	Electronic, Manual or Both
Lawful Basis	What is the lawful basis used to justify the holding and processing of this data. For personal data this needs to be a valid reason under either the GDPR or the Data Protection Bill.
Business Criticality	A ranking of how essential the information asset is, and the disruption that could be caused by its loss or compromise
Location	Where is this data physically stored? For example, on a local computer, in the central College system, on an offsite server
Created By	Who is entering this record into the Information Asset Register
Retention Schedule	How long is the information kept for, and what is the process for identifying information that is no longer needed and securely destroying it? You may wish to consult the College's retention schedule for guidance on how long certain records should be retained
Earliest Record	Date of the oldest record which shouldn't be within the range of (present day minus retention period)
Latest Record	Date of the last record for information assets which are no longer to be updated

Information Asset Owners will also need to have an understanding of the following :

- *Responsible Department* Which department is accountable for this information asset? (Most likely the department of the 'information owner')

- *Who has access to this asset?* Please describe briefly the group of people who have access to this information asset – e.g. staff in a particular team, all staff in a Faculty. It is particularly important to note if any non-College employees have access to the data held on this information asset.

- *How is the information kept secure?* Please provide a brief description of how the information is kept secure (e.g. is access password protected, are paper records containing sensitive data kept in a locked filing cabinet and how are the keys stored?) NB. Don't write down your password or the location of your keys here!

Back-up, Resilience and Disaster Recovery arrangements What arrangements are in place to recover data and/or maintain functionality in case of loss or corruption of data / system(s), including disaster level events.

Version History

Version/Status	Release Date	Comments
0.4/Draft	March 2016	Prepared and submitted by Ros Whiteley for review by Jon Neilson, Jon Hancock and Mike Russell
0.5/In Review	June 2016	Revised version by Okan Kibaroglu; definitions of Information Asset and Information Asset Register added; the concept of information asset entries changed to logical collections of information rather than media. Reviewed by John Neilson, College Secretary and Mike Russell, CIO
0.6/In Review	July 2016	Reviewed by IGSG.
1.0/Approved	16 December 2016	Published on Secretariat's web site
1.1/In Review	November 2017	Pre-GDPR review by Okan Kibaroglu and Tim Rodgers; the title has been changed from Information Security Risk Assessment to Data Protection Impact Assessment.
1.2/In Review	March 2018	Final draft for IGSG review
2.0/Approved	May 2018	Published version