1. INTRODUCTION

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

It governs the use of the Information Asset Register (also referred to as the “IAR”), and the requirement for Information Asset Owners (also referred to as “IAOs”) to register, and maintain the registration of, their information assets in the IAR.

2. KEY TERMS

The following key terms have been defined in the Information Governance Policy Framework and are of particular relevance in this Code of Practice:

Information Asset

Information which satisfies each of the following criteria will qualify as an “information asset” for the purposes of asset registration and must have an entry in the College Information Asset Register:

- the information contains personal data and/or sensitive personal data relating to an identifiable or potentially identifiable natural living person or persons;

- the information is intended to be kept for more than 6 months or may be kept for less than 6 months but could still represent a significant risk to the College if a data breach occurred; and

- each record within the information, whether in digital or physical format, will have shared purpose, risk profile, and risk mitigation measures that make the information a logical collection of data.

There must be a lawful basis within the meaning of the General Data Protection Regulation (GDPR) for the processing of any personal data and/or sensitive personal data within each information asset. Collection of personal data or sensitive personal data without a lawful basis for the collection is not permitted.

The following are some examples of information assets:

- a database of staff personal details or a database of students’ details;
- a database (in physical or electronic format) containing newsletter subscribers’ contacts details;
- PRDPs are collectively a single information asset, but managed across multiple departments. They should be subject to the same rules and owned, collectively, by an Information Asset Owner from Human Resources.

Information Asset Owner

IAOs are senior/responsible individuals working in a relevant business area. Their role is to understand what information is held within their business area, what is added and what is removed, how information is moved, who has access and why. As a result
they are able to understand and address risks to the information that information is used within the law and in line with the College’s objects, and provide written input to the College’s Senior Information Risk Owner (currently, this is the College’s Secretary) annually on the security and use of their information assets.

An IAO will be responsible for an information asset in terms of:

- identifying risks associated with the information asset;
- managing and operating the asset in compliance with policies and standards; and
- ensuring controls implemented manage all risks appropriately.

More details on the role of the IAO can be found at Appendix B to this Code of Practice.

Information Asset Administrator

Information Asset Administrators (also referred to as “IAAs”) work on a day-to-day basis with information contained in an information asset. They have day-to-day responsibility for the asset, and make sure that policies and procedures are applied and adhered to by staff and can recognise actual or potential security incidents relating to their information asset. They are responsible for reporting such incidents to their IAO and consulting the IAO on incident management. The role is flexible and is expected to be performed in addition to existing duties. It is possible that the IAO of an information asset is also the IAA of that asset.

3. USE OF THE INFORMATION ASSET REGISTER

3.1 The IAR procured by the College is an information asset register system called Flowz. This will be the single point of reference for all information assets with data protection significance held across College. A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the personal data within an information asset transmitted, stored or otherwise processed will have compliance and reputational consequences for the College. The IAR is therefore a tool that is envisaged to assist the College’s data protection compliance processes.

3.2 Information Asset Owners must:

- when creating an asset record, ensure that all information asset attributes are completed, seeking advice from ICT, the Archives and Corporate Records Unit or the Data Protection Officer where necessary;
- make sure the asset record is up-to-date and comprehensive – Appendix A to this Code of Practice indicates the type of information that will need to be input into the system;
- ensure that access records are maintained on the IAR;
- identify all interested parties in the proper-management of their asset (e.g. administrator, representative of the data processor (if applicable) etc…);
- upload documents where required (e.g. training records, local policies);
- when DPIA functionality is enabled within Flowz, conduct the regular DPIA review (see https://www.imperial.ac.uk/admin-services/legal-services-office/data-protection/dataassessments/). They should attend IAO training
sessions to ensure they have a good understanding of the IAR and update themselves on any legislative and policy developments relevant to information governance.

3.3 The IAR:

- is cloud based and can be accessed via the College’s Single Sign On facility which can be accessed by copying and pasting this url address in your browser (just clicking on the link will not open the relevant web page): https://imperial.flowz.co.uk/Account/SSOLogon;
- each information asset should have an allocated IAR and an IAA. The owner and administrator can, if necessary, be the same person;
- the system only permits a single IAO to be recorded against information assets. An IAO can own more than one information asset;
- can provide reports on ownership, risk and other metrics.

3.4 Ongoing viability

- If an IAO leaves the College they should ensure they hand over their IAO responsibilities ahead of their departure, ensuring their successor is able to access the IAR.
- Where no Information Asset Owner exists, ICT Governance will assume the role of IAO pending the allocation to an appropriate candidate in the appropriate faculty or department
- The product is supported by ICT Service Desk. Calls should be logged in the normal manner where they will be triaged. The system is supported internally by Facilities and Place within ICT, with escalation to the supplier, Flowz.

APPENDIX A: STRUCTURE OF INFORMATION ASSET REGISTER

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Asset Owner</td>
<td>Who is responsible for the information stored in this information asset, and is the point of contact for queries about this information asset?</td>
</tr>
<tr>
<td>Information Asset Administrator</td>
<td>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.</td>
</tr>
<tr>
<td>Name of the Information Asset</td>
<td>A unique name for the information asset</td>
</tr>
<tr>
<td>Description of the Information Asset</td>
<td>Please provide a brief description of the information asset. Where possible, please provide a brief overview of the kinds of information held.</td>
</tr>
<tr>
<td>Status</td>
<td>IAR field only – Temporary, Approved or Inactive</td>
</tr>
</tbody>
</table>
### Classification

- **Does the asset contain sensitive data? What are the risks associated with this data and how are they mitigated?**
  
  Sensitive data includes:
  
  - Commercially sensitive administration or research data
  - Sensitive personal data (also known as special categories of personal data), as defined in the General Data Protection Regulation. This encompasses personal data related to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of unique identification, health, sex life or sexual orientation
  - Personal financial data
  - Patient Identifiable Data held for research purposes
  - 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.

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Electronic, Manual or Both</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lawful Basis</td>
<td>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.</td>
</tr>
<tr>
<td>Business Criticality</td>
<td>A ranking of how essential the information asset is, and the disruption</td>
</tr>
</tbody>
</table>
that could be caused by its loss or compromise

<table>
<thead>
<tr>
<th>Location</th>
<th>Where is this data physically stored? For example, on a local computer, in the central College system, on an offsite server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created By</td>
<td>Who is entering this record into the Information Asset Register</td>
</tr>
<tr>
<td>Retention Schedule</td>
<td>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</td>
</tr>
<tr>
<td>Earliest Record</td>
<td>Date of the oldest record which shouldn’t be within the range of (present day minus retention period)</td>
</tr>
<tr>
<td>Latest Record</td>
<td>Date of the last record for information assets which are no longer to be updated</td>
</tr>
</tbody>
</table>

*Information Asset Owners will also need to have an understanding of, and enter, the following information into the Information Asset Register:*

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

- **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?
APPENDIX B: ROLE OF INFORMATION ASSET OWNER

The role of the Information Asset Owner (IAO) is a vital part of protecting and maximising the efficient use of information in College. The main purpose of the role is to understand and address risks to the information they ‘own’, usually as part of their management of the service. It also provides assurance to the Senior Information Risk Owner (SIRO) on the security and use of these assets.

SPECIFIC RESPONSIBILITIES

The College has adopted the concept of an Information Asset Owner (IAO) as defined by the Cabinet Office in respect of Information Asset Owners in UK government departments; this is as follows:

“Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result, they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process.”

Specifically, this means that IAOs:

- lead and foster a culture that values, protects and uses information for the public good;
- undertake and pass information governance training and maintain a high degree of awareness of the legal framework;
- understand and address risks to the asset and provide assurance to the SIRO;
- maintain understanding of ‘owned’ assets and how they are used;
- observe compliance with the provisions of the General Data Protection Regulation in respect of personal data;
- approve information transfers only to achieve business purposes avoiding unnecessary data moves and duplication;
- approve and oversee the disposal mechanism of the information when it is no longer needed;
- know what information the asset holds and who has access to the asset and why; define the process and approval mechanism of how access is authorised and oversee that these requests are logged;
- abide by and enforce compliance with the Imperial College Information Security Policy in relation to the information asset they own;
- undertake regular reviews on the information risks associated with the asset as described in this Code of Practice;
- employ ICT’s Change Management process for any changes made to information assets managed by ICT.

1 From the Cabinet Office document ‘Guidance on the IAO role’