Records Management Policy
(including Information Classification)

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>University Secretary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Approval Date</td>
<td>4 June 2013</td>
</tr>
<tr>
<td>Reviewed</td>
<td>May 2017</td>
</tr>
<tr>
<td></td>
<td>May 2019</td>
</tr>
<tr>
<td>Review Date</td>
<td>May 2022</td>
</tr>
</tbody>
</table>
1 Introduction

1.1 Records management is essential for the efficient conduct of business and adherence to legal obligations. The University is committed to establishing and maintaining good records management ensures it retains important information while also ensuring that data no longer required is disposed of in line with its obligations under Data Protection legislation. A robust records management process also ensures that the University can fulfill disclosure requirements to data subjects and also under the Freedom of Information Act (2000).

1.2 The University holds a wide variety of information that must be protected against unauthorised access. Information classification which is included in this policy ensures that staff make decisions in relation to the retention of information and who can access it in line with the University’s information classification system.

2 Scope

2.1 This policy applies to all information produced or provided to the University.

3 Related policies

3.1 This Policy supplements the University’s Data Protection Policy and should be read in conjunction with it. It should also be read in conjunction with the Information Security Policy and guidance on email usage.

4 Records

4.1 Records can be defined as ‘Information created, received and maintained as evidence and information by an organisation or person in pursuance of legal obligations or in the transaction of business’.

4.2 Records are an essential resource and contain information which is unique and invaluable. They can be used as an audit trail as they provide evidence/proof of a specific activity. Records come in electronic (including emails, video and audio materials) and paper format. It is important that both types must be managed equally well, especially in terms of storage, accessibility and disposal.

4.3 Records should be managed accordance with the principles below:

- **Records**: Records are evidence of our actions and decisions and must be retained as long as required.
- **Responsibility**: All staff have responsibility for Records and should be aware of what they are using and creating and how they should be retained;
- **Risk**: There are significant risks from loss, damage or unauthorised access which need to be managed effectively. There are also risks from loss of control of records;
- **Retention**: Keep records only as long as they are needed;
Rights
Staff, students and others have the rights under data protection legislation. The public has a right to access our records subject to data protection regulations and Freedom of Information exemptions;

Reliability
Records should be managed effectively to ensure that they are high quality and reliable.

5 Retention Schedule

5.1 A properly implemented and consistently applied Records Retention Schedule improves the efficiency of working practices, and protects the interests of the University by ensuring that records are not kept for longer than they are needed to meet operational needs.

5.2 The purposes of the Retention Schedule are to:

- Improve efficiency of working practices and enable easy and speedy retrieval of records;
- Prevent records from being discarded prematurely;
- Ensure that information is not kept unnecessarily;
- Eliminate retention of duplication of records;
- Provide a consistent, controlled system for the disposal of material across the University;
- Help in saving space, time, effort and money;
- Comply more readily with requests for information, both internally and externally (e.g. request made under Data Protection Legislation or the Freedom of Information Act 2000).

5.2 The University does not keep all records permanently. Only records which have, evidential, legal, historical, or business importance are retained for a specific length of time or permanently (in limited cases). The time periods for retention are outlined in the retention schedule.

5.4 Multiple copies of records should not be retained. Extraneous copies of paper documents are to be disposed of. Where these include personal data or confidential information these should be disposed of securely in confidential waste bin or shredded. Only one copy of the document is therefore retained for retention purposes. This also applies to emails. Key emails should be retained and care taken to establish which should be maintained and which deleted.

6 Classification of Information

6.1 Different types of information require different protection measures against unauthorised access. The classification of records within the Retention Schedule helps staff responsible for records determine what information should and should not be disclosed to those both inside and outside the University.

6.2 The records should be classified as follows:
Public information which the University chooses to put into the public domain

Internal information which, while there may be no risks in making it public are not intended for wide circulation

Confidential information for which there is a medium risk when disclosed and which should be accessed by authorised University Staff only

Strictly Confidential information where there is a high risk when disclosed because of it being special category data or commercially confidential and to which access must be highly restricted.

6.3 Appendix 1 gives examples of classifications. Information which is classified as confidential or strictly confidential should only be shared in accordance with the Information Security Policy.

7 Staff Responsibilities

7.1 The University Secretary and Chief Compliance Officer and Information Security Manager have responsibility for ensuring an appropriate records management framework and providing guidance.

7.2 Heads of Schools and Professional Departments have overall responsibility for the management of records generated by activities within their departments, ensuring that they are properly maintained and that access is only as authorised.

7.3 The Head of HR and the Chief Information Officer and Associate PVC have particular responsibility to ensure the integrity of the staff and student records respectively. The Director of Alumni and Development is responsible for managing alumni records and those of donors while the Head of Admissions is responsible for applicant data. The Chief Financial Officer is responsible for the integrity of financial records.

7.4 All staff that create, receive and use documents have record management responsibilities. Each member of staff is responsible for ensuring that records within their control are kept in accordance with the retention schedule and that they are not disclosed unless authorised.

7.5 All staff should be aware that they are creating records through their work and ensure that these are secured and disposed of appropriately, including emails. They should establish which emails are key records and act accordingly.

8 Format of Retention Schedule

8.1 The Retention Schedule which forms part of this Policy has been prepared to assist in the effective management of records by identifying types of documents held by each School/College and Professional Services which require retention, setting out the retention period for each type of document, who is responsible and the reasons for keeping it.
8.2 The Records Retention Schedule is organized by class. The classifications relate to the JISC Business Classification Scheme which has been adapted as appropriate. In each class a list of records associated with the business function responsible for the class is provided, along with the retention period applicable to each record, and the justification relating to the retention period and the information classification of the record.

8.3 The retention periods are independent of format and therefore apply to any medium whether paper or electronic records.

8.4 There is an “Owner of Records” category which identifies the head of each School, Department or Support Service who has overall responsibility for the management and disposal of the record. The Owner of the Record is responsible for the implementation of the Retention Policy within their area of responsibility must ensure that records are managed in accordance with the schedule and disposed of when required on an annual basis.
### Appendix 1

<table>
<thead>
<tr>
<th>Classification</th>
<th>Risk and access</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>No risk</td>
<td>Prospectus</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Opening times</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Open day information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Published research</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vacancy details</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Staff directory</td>
</tr>
<tr>
<td>Internal-</td>
<td>Low – disclosure to third parties could be inappropriate. Should only be accessed by University staff</td>
<td>Internal emails</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minutes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Communications</td>
</tr>
<tr>
<td>Confidential</td>
<td>Medium to high - Inappropriate disclosure could cause reputational damage and breach contractual and legal obligations. Only accessible to those who need to know as part of their job role</td>
<td>Documents containing personal data, employee and student records, sensitive business data, financial data</td>
</tr>
<tr>
<td>Strictly confidential</td>
<td>Very high - Inappropriate disclosure would cause significant reputational damage and liable to result in fines, breach of contract and other legal obligations. Only accessible to those who need to know as part of their job role – personal data should be encrypted.</td>
<td>Special category data – including medical, disability and ethnicity data, business critical information, University banking information</td>
</tr>
</tbody>
</table>