Information Handling Policy
<table>
<thead>
<tr>
<th><strong>Policy Version:</strong></th>
<th>1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy Review Interval:</strong></td>
<td>Annually by the ISG from the date of authorisation</td>
</tr>
<tr>
<td><strong>Author:</strong></td>
<td>Director of LISD</td>
</tr>
<tr>
<td><strong>Authorised By:</strong></td>
<td>Information Security Group</td>
</tr>
<tr>
<td><strong>ISG Group Members:</strong></td>
<td>Director of Estates and Campus Services (Chairperson)  Director of Library and Information Services Division  LISD IT and Development Manager  Head of IT Infrastructure Services  Data Protection Officer</td>
</tr>
<tr>
<td><strong>Authorisation Date:</strong></td>
<td>March 2014</td>
</tr>
</tbody>
</table>
1. Introduction
This Information Handling Policy is a sub-policy of the Information Security Policy and sets out the requirements relating to the handling of the College’s information assets. Information assets must be managed in order to protect against the consequences of breaches of confidentiality, loss of integrity, interruption to availability, and non-compliance with legislation which would otherwise occur.

2. Inventory and ownership of information assets
An inventory of the College’s main information assets will be developed by December 2014 and reviewed annually. Each category will have nominated owners who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.

3. Security classification
Each information asset category will be assigned a security classification by the asset owner which reflects the sensitivity of the asset according to the following classification scheme:

- Public – available to any member of the public without restriction.
- Open – available to any authenticated member of the College.
- Confidential – available only to specified members, with appropriate authorisation.
- Strictly Confidential – available to only a very small number of members, with appropriate authorisation.
- Secret – the most restricted category. It is not anticipated that many College assets will be assigned this classification.

Any information which is disclosable under the Freedom of Information Act 2000 will be classified as public. Any data which is classified as sensitive personal data under the Data Protection Act 1998 (or its successor legislation) will be classified as strictly confidential. Any information which is not explicitly classified will be classified as open, by default.

4. Access to information
Members of the College will be granted access to the information they need in order to fulfil their roles within the College. Members who have been granted access must not pass on information to others unless the others have also been granted access through appropriate authorisation.

5. Disposal of information
Great care needs to be taken to ensure that information assets are disposed of securely. Confidential paper waste must be disposed of in accordance with formal College procedures (which are documented on the College’s Sustainability website).

Electronic information must be securely erased or otherwise rendered inaccessible prior to leaving the possession of the College, unless the disposal is undertaken under contract by an approved contractor.

In cases where a storage system is required to be returned to a supplier it should be securely erased before being returned unless contractual arrangements are in place with the supplier which guarantee the secure handling of the returned equipment. If this is not possible, then the storage system should not be returned to the supplier and should remain in the possession of the College until it is disposed of securely.
6. **Removal of information**

College data which is subject to the Data Protection Act or which has a classification of confidential or above should be stored using College facilities or with third parties subject to a formal, written legal contract with the College, wherever possible. In cases where it is necessary to otherwise remove data from the College, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss. Strictly confidential data in electronic form must be strongly encrypted prior to removal. Secret data must never be removed except with the explicit written permission of the data owner.

Particular care needs to be taken when information assets are in transit. College supplied mobile devices must always be fully encrypted by IT Helpdesk staff.

7. **Using personally owned devices**

Data subject to the Data Protection Act must never be stored on personally owned devices. Data classified as sensitive under the Data Protection Act must neither be stored on nor processed using personally owned devices.

Personally owned devices should not be used for the storage or processing of any other information classified as strictly confidential or above without the explicit written permission of the data owner. Appropriate security measures must be taken when using personally owned devices to process or store any College data.

8. **Information on desks, screens and printers**

Members of staff who handle confidential paper documents should take appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times.

Care should also be taken when printing confidential documents to prevent unauthorised disclosure. Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons and all computers should be locked while unattended. Staff offices should be locked when empty.

9. **Backups**

Information owners must ensure that appropriate backup and system recovery measures are in place. Where backups are stored off site, appropriate security measures must be taken to protect against unauthorised disclosure or loss. Recovery procedures should be tested on a regular basis. Information which is entrusted to the care of IT Services will meet these requirements.

10. **Exchanges of information**

Whenever personal data or other confidential information is transmitted to or exchanged with other organisations, appropriate information security measures must be established to ensure the integrity and confidentiality of the data transferred. Regular exchanges must be covered by a formal written agreement with the third party.

Information classified as strictly confidential may only be exchanged electronically both within the College and in exchanges with third parties if the information is strongly encrypted prior to exchange. Information classified as secret may not be transmitted electronically except with the explicit written permission of the information owner.
When exchanging information by email or fax, recipient addresses should be checked carefully prior to transmission.

Unsolicited emails, faxes, telephone calls, instant messages or any other communication requesting information which is not classified as public should not be acted upon until and unless the authenticity and validity of the communication has been verified.

Members of the College must not disclose nor copy any information classified as confidential or above unless they are authorised to do so.

11 Reporting losses
All members of the College have a duty to report the loss, suspected loss or unauthorised disclosure of any College information asset to the Director of the Library & Information Services Division.