Information Management

Good information management ensures that the University gains maximum benefit from information and protects its information assets from harm while fulfilling its legal and contractual obligations by balancing:

- **Confidentiality** – protecting information against unauthorised access.
- **Integrity** – preventing unauthorised tampering or destruction of information assets.
- **Availability** – ensuring that information is made available as and when needed for the University to conduct its business properly and without delay.

Information assets must be identified and classified [1] in a way that promotes effective management based on the level of risk associated with each type of asset.

<table>
<thead>
<tr>
<th>Category</th>
<th>Summary</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>Information intended for the public domain or that carries no appreciable confidentiality or integrity risk.</td>
<td>All information is assumed to be open unless specifically designated otherwise.</td>
</tr>
</tbody>
</table>
| Restricted | Information intended for a defined audience but not particularly sensitive. | • Committee minutes (except Council and Senate).           
• Draft discussion papers  
• Intranet web sites  
• Most internal documents |
| Confidential| Information likely to cause significant harm to the University’s reputation, assets or ability to meet its legal and contractual obligations if revealed outside of the intended audience. | • Legally privileged documents  
• Senior Management and Strategic discussion papers  
• Live examination papers  
• Student assessments, results  
• Contracts and commercial in confidence information.  
• Student recruitment and admissions data.  
• Unpublished research (if sensitive)  
• University budget / TRAC data  
• Sensitive personal information / Data Protection Act 1998  
• Salary and Payroll data  
• Patient identifiable data  
• Third party commercial data  
• Credit / payment card details |

It is expected that most information assets will be ‘Open’ or ‘Restricted’ and that ‘Confidential’ will be by far the smallest category.

Information is abstract so these guidelines concern ‘information assets’ where information is instantiated in physical or electronic form. The level of risk associated with information assets may vary with time, some may be confidential until they reach a certain stage in their lifecycle and then become open (e.g. examination papers, research data).

Responsibilities

**Information Asset Owners**

Information Asset Owners (IAO) – managers and others responsible for defined information assets establish local procedures and issue guidance on classifying different kinds of information assets based on risk levels and ensure that critical assets are documented in Information Asset Registers.

**All**

University staff, and some students and others as appropriate, adhere to the relevant codes of practice, policies and standards together with procedures and guidelines issued by the asset owners and IT Services.
Handling Summary

Email
1. Encrypt email containing **Confidential** information or with **Confidential** attachments.
2. Sign email to protect against tampering (but no need to sign encrypted email).

Email encryption and signing should be used sparingly and only when necessary using the University secure email facility. Microsoft Outlook users should click on the ‘traffic light’ buttons where available.

Storage
1. Encrypt **Confidential** data except when stored in a central University data store in a secure network zone and not accessible from outside the University.
2. Do not encrypt **Restricted** so that it can be scanned for viruses and other malware.
3. Avoid storing **Confidential** data on laptops, desktops, mobile devices and removable media else ensure it is encrypted.

File Transfer
1. Encrypt **Confidential** data using FTPS (preferred) or SFTP including ‘local’ file transfers within the University’s own network.

Remote Access
1. Encrypt access to **Restricted** or **Confidential** web applications and pages using HTTPS.
2. Access University email from encrypted University laptops, use Outlook Web Access (OWA) or ‘Good for Enterprise’ for mobile devices.
3. Use 2-factor authentication and VPN to access **Confidential** data and core business applications.

Cloud Storage
1. Encrypt **Confidential** data using a product that conforms to the Cryptography Standard [2].
2. Ensure physical storage is within UK or EEA or the supplier is Safe Harbour certified.

Fax
1. Do not fax **Confidential** information unless a trusted person is standing by at the other end to receive it.

Hard Copies / Paper Documents
1. If **Confidential**, mark on every page.
2. If **Restricted**, mark at least on front page or exterior surface.
3. Store **Confidential** papers in a locked cabinet with known key holders.

Destruction
1. If **Confidential**, shred paper copies (preferably cross-cut) or use the University’s secure disposal service.
2. Delete **Confidential** files and overwrite removable media using an approved utility.

Mobile Devices
1. Encrypt **Confidential** data on mobile devices using a product that conforms to the Cryptography Standard [2].
2. Use ‘Good for Enterprise’ or Outlook Web Access (OWA) for accessing University email on mobile devices.

Other Markings

<table>
<thead>
<tr>
<th>Category</th>
<th>Equivalents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>Public, Unrestricted</td>
</tr>
<tr>
<td>Restricted</td>
<td>Internal use only</td>
</tr>
<tr>
<td>Confidential</td>
<td>Commercial in confidence, Private and confidential, Personal</td>
</tr>
</tbody>
</table>

Further Information
If you have any questions or comments concerning this document, please contact IT Services at itsecurity@contacts.bham.ac.uk or consult the following referenced documents:

1. Information Classification Standard [2]

http://www.it.bham.ac.uk/policy/