## Information Security policy

<table>
<thead>
<tr>
<th>Document Filename</th>
<th>Information Security Policy.docx</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Information Classification</td>
<td>Open</td>
</tr>
<tr>
<td>Status</td>
<td>Approved</td>
</tr>
<tr>
<td>Date</td>
<td>18 December 2015</td>
</tr>
<tr>
<td>Policy owner</td>
<td>Graham McKay</td>
</tr>
<tr>
<td>Policy contact</td>
<td><a href="mailto:g.mckay@dundee.ac.uk">g.mckay@dundee.ac.uk</a></td>
</tr>
</tbody>
</table>
Document Approval

<table>
<thead>
<tr>
<th>Title/Role</th>
<th>Name of Approver(s)</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Management Committee</td>
<td>Jim McGeorge, Paul Saunders, Ian Leith, Richard Parsons, Wesley Rennison, Andrew Hewitt, Tim Hustler.</td>
<td>18/12/2015</td>
</tr>
</tbody>
</table>

Version Control

<table>
<thead>
<tr>
<th>Revision</th>
<th>Status</th>
<th>Author(s)</th>
<th>Reviewed By</th>
<th>Approved By</th>
<th>Issue Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Draft</td>
<td>Graham McKay</td>
<td></td>
<td></td>
<td>03/04/2015</td>
</tr>
<tr>
<td>0.2</td>
<td>Draft</td>
<td>Graham McKay</td>
<td>Richard Parson Alan Bell</td>
<td></td>
<td>07/09/2015</td>
</tr>
<tr>
<td>1.0</td>
<td>Approved</td>
<td>Graham McKay</td>
<td>Richard Parsons Alan Bell</td>
<td>Information Management Committee</td>
<td>18/12/2015</td>
</tr>
</tbody>
</table>
## Contents

1. Document overview .................................................................................................................. 1
  1.1. Purpose ................................................................................................................................. 1
  1.2. Scope .................................................................................................................................... 1
  1.3. Definitions ............................................................................................................................. 1
  1.4. References ............................................................................................................................ 1
2. Policy ............................................................................................................................................. 3
3. Review ........................................................................................................................................... 4
4. Breaches of policy ......................................................................................................................... 4
5. Further information ...................................................................................................................... 4
1 Document overview

1.1 Purpose

1.1.1 Purpose of this policy is to safeguard University of Dundee information from security threats that could have an adverse effect on its operations or reputation, whilst fulfilling its duty of care towards the information that it has been entrusted with. This is achieved by protecting the confidentiality, integrity, availability and value of information through the use of optimal controls.

1.2 Scope

1.2.1 This policy will apply to all information processed, accessed, manipulated or stored by the University of Dundee whether owned or managed and is applicable to all staff, students and visitors.

1.3 Definitions

1.3.1 University – The University of Dundee is a Scottish Registered Charity, No. SC01509 with its registered office at Tower Building, Nethergate, Dundee DD1 4HN.

1.3.2 Staff - Staff are salaried members of the University or contracted individually by the University to provide a service.

1.3.3 Student - a person pursuing any course of study in the University.

1.3.4 Visitors - A visitor is anyone, not a member of staff or student, requiring access to University premises or services.

1.3.5 Information - The result of processing, manipulating, or organising data. Examples including but not limited to, text images, sounds, codes, computer programmes, software and databases.

1.3.6 Data - Information in raw form.

1.3.7 Confidentiality\(^1\) - property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

1.3.8 Integrity\(^2\) – property of accuracy and completeness.

1.3.9 Availability\(^3\) – property of being accessible and usable upon demand by an authorized entity.

1.4 References

1.4.1 University of Dundee Risk Management Strategy.


---

\(^1\) ISO/IEC 27000:2014 - 2.12
\(^2\) ISO/IEC 27000:2014 - 2.40
\(^3\) ISO/IEC 27000:2014 - 2.9
2 Policy

2.1.1 The University of Dundee is committed to protecting the security of its information and information systems. It is also committed to a policy of education, training and awareness for information security and to ensuring the continued business of the University.

2.1.2 It is the University of Dundee’s policy that the information it manages shall be appropriately secured to protect against breaches of confidentiality, failures of integrity or interruptions to the availability of that information and to ensure appropriate legal, regulatory and contractual compliance.

2.1.3 To determine the appropriate level of control that should be applied to information, a risk-based approach will be utilised to ensure residual risk is aligned to the University’s risk appetite.

2.1.4 An Information Security Steering Group (ISSG) is established to oversee information security within the Organisation and to formulate and disseminate information security policies, procedures and guidelines that, subject to senior management approval, all staff, students and visitors are required to comply with.

2.1.5 Information security awareness and training will be available to all staff and students.

2.1.6 Specialist advice on information security shall be made available throughout the University and advice can be sought via the University’s Information Security Team.

2.1.7 Actual or suspected information security incidents should be reported promptly to End User Services who will allocate the incident to an appropriate member of staff who will manage the incident to closure, and analyse it for lessons to be learnt.

2.1.8 Where a suspected or actual breach involves personal data, it must be reported for thorough investigation to the University’s Data Protection Officer.

2.1.9 Records of the number of security breaches and their type should be kept and reported on a regular basis to the Senior Management Team and the Audit Committee.
3 Review

3.1.1 The Information Security Steering Group is responsible for keeping this policy current. This policy will be reviewed annually or more frequently as required.

4 Breaches of policy

4.1.1 Failure to comply with this policy may result in disciplinary action being taken against you under University of Dundee disciplinary procedures, which may include summary dismissal. If there is anything in this policy that you do not understand, please discuss it with your line manager.

5 Further information

5.1.1 If you have any questions regarding this policy, please contact the Chief Information Security Officer at g.mckay@dundee.ac.uk.