Information Security Policy

Document Summary

<table>
<thead>
<tr>
<th>Document ID</th>
<th>Information Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Approved</td>
</tr>
<tr>
<td>Information Classification</td>
<td>Public</td>
</tr>
<tr>
<td>Document Version</td>
<td>1.0 – May 2017</td>
</tr>
</tbody>
</table>
1. Introduction

1.1. As a centre of knowledge and training, Royal Holloway University London (RHUL) focuses on exploiting information. Next to people, information is RHUL’s most important asset. The information we use exists in many forms: printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Regardless of the form it takes, or means by which it is shared or stored, information should always be protected appropriately.

1.2. Information security is characterized here as being concerned with guaranteeing availability (ensuring that authorized users always have access to information when they need it), integrity (safeguarding its accuracy and completeness), confidentiality (ensuring that sensitive information is accessible only to those authorized to use it), and authenticity. It must also address proper methods of disposal of information that is no longer required. Security is essential to the success of almost every academic and administrative activity. Effective security is achieved by working within a proper framework, in compliance with legislation and RHUL’s policies, and by adherence to approved procedures and codes of practice.

1.3. The objectives of this information security policy are to:

1.3.1 ensure that all of RHUL’s computing facilities, programs, data, network and equipment are adequately protected against loss, misuse or abuse, and that this protection is cost-effective;

1.3.2 ensure that all users are aware of and fully comply with this policy statement and all associated policies, and are aware of and work in accordance with the relevant procedures and codes of practice;

1.3.3 ensure that paper records are kept securely and managed effectively;

1.3.4 ensure that all users are aware of and fully comply with the relevant UK and European Union legislation;

1.3.5 create across RHUL an awareness that appropriate security measures must be implemented as part of the effective operation and support of information management systems;

1.3.6 ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle;

1.3.7 ensure that information is disposed of in an appropriately secure manner when it is no longer relevant or required.

1.4. The policy applies to all staff and students of RHUL and all other computer, network or information users authorized by RHUL or any department or faculty
thereof. It relates to their use of any RHUL-owned facilities (and those leased by or rented or on loan to RHUL), centrally managed or otherwise; to all private systems (whether owned, leased, rented or on loan) when connected to the RHUL network; to all RHUL owned or licensed data and programs (wherever stored); and to all data and programs provided to RHUL by sponsors or external agencies (wherever stored). The policy also relates to paper files and records created for the purposes of RHUL business.

1.5. Definitions of the terms used in this policy statement and supporting documentation may be found in the glossary in the Glossary of Terms.

1.6. The RHUL Senior Management Team has approved this policy statement and delegated its implementation to Heads of Departments.

1.7. Those requiring information, explanation or training about any aspects of the policy which relate to computer security should discuss their needs with the RHUL IT Department. Questions about the creation, classification, retention and disposal of records (in all formats) should be taken to the Data Steward. The RHUL Head of Information Security and the Data Protection Officer will in the first instance be responsible for interpretation and clarification of the information security policy.

2. Responsibilities for Information Security

2.1. All who make use of RHUL’s systems and information have responsibility for protecting those assets. Individuals must, at all times, act in a responsible and professional way in this respect, and will refrain from any activity that may jeopardize security.

2.2. The Information Technology Strategic Board (IT SIB) is responsible for defining an information security policy and for ensuring it is discharged by all academic and professional services departments and faculties through the respective Head of Department. The policy will apply to associate bodies e.g. RHUL owned companies and the Students’ Union.

2.3. Heads of Department are required to implement this policy in respect of both paper and electronic systems operated by their Departments and are responsible for ensuring that staff, students and other persons authorized to use those systems are aware of and comply with it and associated codes of practice. Heads of Department should ensure adequate oversight of security (in consultation with the RHUL Head of Information Security), through central and departmental IT support staff or otherwise.

2.4. The Infrastructure and Security Group (ISAG) advises the SIB on matters related to compliance with this policy, and is responsible for regularly reviewing it for completeness, effectiveness and usability. The SIB, in collaboration with the Infrastructure and Security Working Group and the RHUL Head of Information
Security, will from time to time make available supplementary procedures and codes of practice, and promote them throughout RHUL; once approved by the IRGG these will also become RHUL policy and will be binding on departments.

The ISAG will also arrange for analysis of security assessments received from departments, and report on these to the SIB.

2.5. The RHUL Head of Information Security, in addition to their involvement in policy making, provides relevant operational services. These include incident response and coordination, dissemination of security information, training, consultancy, and liaison with other external security teams and law enforcement agencies.

2.6. It is the responsibility of each individual to ensure his/her understanding of and compliance with this policy and any associated procedures or codes of practice.

2.7. Staff with supervisory responsibility should make their supervised staff or students aware of best practice.

2.8. Staff and students who process or who are responsible for the processing of personal data, as defined in RHUL’s Data Protection Policy, are additionally required to understand and comply with all obligations placed upon them under agreements with external parties, including but not limited to information security, integrity and perpetual confidentiality.

3. Compliance with Legislation

3.1. RHUL, each member of staff, and its students have an obligation to abide by all UK legislation and the relevant legislation of the European Union. Of particular importance in this respect are the Computer Misuse Act 1990, the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000, the Terrorism Act 2006 and the Counter Terrorism and Security Act 2015.

The Seventh Principle of the Data Protection Act 1998 requires that organisations take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Organisations are also required to ensure a level of security appropriate to the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and the nature of the data to be protected.

3.2. Relevant legislation is referenced in supporting polices and guidelines. Full texts are available from The Stationery Office and at:


4. Risk Assessment and Security Review by Departments
4.1. Information should be suitably classified according to the guidance given in “Data Management Policy”.

Stewards should adopt a risk-based approach to assessing the value of information handled, its sensitivity, the potential damage or distress caused by a loss of the information and the appropriateness of technological, organisational and physical security controls in place or planned. Without proper assessment of the value of information assets, and the consequences (financial, reputational and otherwise) of loss of data or disruption to service, efforts to improve security are likely to be poorly targeted and ineffective. Reviews should be conducted on an annual basis, to take into account changes to technology, legislation, business requirements and priorities and at the point of new data being assigned to the Data Steward. Security arrangements should be revised accordingly.

5. Breaches of Security

5.1. Any individual suspecting that the security of a computer system has been, or is likely to be, breached should inform the RHUL Head of Information Security immediately. RHUL ISG will advise RHUL on what steps should be taken to avoid incidents or minimize their impact, and identify action plans to reduce the likelihood of recurrence.

5.2. In the event of a suspected or actual breach of security, RHUL Head of Information Security may, after consultation with the relevant Steward or Head of Department, require that any unsafe systems, user/login names, data and/or programs be removed or made inaccessible.

5.3. Where a breach of security involving either electronic or paper records relates to personal data, the RHUL Data Protection Officer must be informed, as there may be an infringement of the Data Protection Act 1998 which could lead to intervention by the Information Commissioner’s Office and potentially civil or criminal proceedings. It is vital, therefore, that users of RHUL’s information systems comply, not only with this policy, but also with RHUL’s Data Protection Policy and associated codes of practice, details of which may be found on the RHUL website.

5.4. All physical security breaches should be reported to RHUL Security.

5.5. IT may monitor network activity, receive reports from the RHUL Head of Information Security and other security agencies, and take action or make recommendations consistent with maintaining the security of RHUL information assets.

6. Policy Awareness and Disciplinary Procedure
6.1. The contract of employment shall state that employees are required to comply with the Information Security Policies, including such additions or amendments thereto as may be made by RHUL from time to time.

6.2. As part of an induction process, Managers are reminded via the standard checklist to ensure that the online information security awareness training is completed.

6.3. Students are required to comply with the Information Security Policies, including such additions or amendments thereto as may be made by RHUL from time to time.

6.4. Existing staff and students of RHUL, authorised third parties, guests, conference delegates and contractors given access to the RHUL network will be advised of the existence of this policy statement and the availability of the associated procedures, codes of practice and guidelines which are published on the RHUL website. Failure of an individual student or member of staff to comply with this policy may lead to the instigation of disciplinary procedures and, in certain circumstances, legal action may be taken. Failure of a contractor to comply could lead to the cancellation of a contract.

7. Supporting Policies, Procedures and Codes of Practice

7.1. Supporting policies, procedures and codes of practice amplifying this policy statement are published with it and are available on the RHUL website. Staff, students, contractors and other third parties authorized to access the RHUL network to use the systems and facilities identified in paragraph (1.4) of this policy, are required to familiarize themselves with these and to work in accordance with them. Guidance notes will also be published to facilitate this.

7.2. Other agencies, such as National Health and Government data agencies may place additional obligations on users of their data. RHUL requires compliance with these.

7.3. Personal data (as defined by the Data Protection Act, 1998) must be stored securely; if such data is held on mobile devices (e.g. Smartphones) or removable media, it must be strongly encrypted, in compliance with the Data Protection Policy and the Data Access Policy. Other forms of sensitive business data, intellectual property, etc. should, similarly, be strongly encrypted. The Head of Information Security will issue and keep under review guidance on what constitutes an acceptable standard of encryption.

7.4. Any outsourced information services must be subject to a documented contract which must comply with the guidelines in 3rd Party Supplier Policy.


8.1. This policy statement does not form part of a formal contract of employment with RHUL, but it is a condition of employment that employees will abide by the
regulations and policies made by RHUL. Likewise, these latter are an integral part of the regulations for students.

*The policy sub documents that make up this document are:*

- Credentials Policy
- Data Access Control Policy
- Physical Access Policy – Data Centre and Communications Cabinet Rooms
- Removable Media Policy
- Secure Build Policy
- Cloud / 3rd Party Code of Practice
- College Acceptable Use Policy
- Change Management Policy
- Incident Management Policy
- Penetration Testing Policy
- Vulnerability Management Policy
- 3rd Party Data Policy
- Asset Ownership Policy
- Data Quality and Consistency Policy
- Data Management Policy
- Data Retention Policy
- IT Patch/Upgrade Policy
- Logging and Monitoring Policy
- Connecting to Campus Network Policy
- Firewall Policy
- IP Allocation and Management Policy
- Remote Access Policy
- RIPA and FOI Policy for IT Services
- Wireless Access Policy
- Mobile Working Policy
- Removable Media Policy
### Revision History

<table>
<thead>
<tr>
<th>Revision date</th>
<th>Summary of Changes</th>
<th>Changes marked</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.12.2016</td>
<td>Initial Draft</td>
<td>N</td>
</tr>
<tr>
<td>February 2017</td>
<td>Updated post workshops and comments from DPO (CC)</td>
<td>N</td>
</tr>
<tr>
<td>May 2017</td>
<td>Version for SIB ratification</td>
<td>N</td>
</tr>
</tbody>
</table>

### Approvals

<table>
<thead>
<tr>
<th>Ratified by PRC</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved by the Strategic IT Board</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Information Security Policy
Classification: Public
Status: Approved