Mobile Working Policy

Incorporating – Bring Your Own Device (BYOD), VPN Policy.

Document Summary

<table>
<thead>
<tr>
<th>Document ID</th>
<th>Mobile Working 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 – July 2017</td>
</tr>
</tbody>
</table>
1. Purpose

This document states the College mobile working rules which include the roles and responsibilities of users, approved mobile working usage, the appropriate controls for mitigating the risks of mobile working and incident reporting.

Mobile working and remote access extends to the transit and storage of information (or operation of systems) outside of the College infrastructure, typically over the Internet. Mobile devices will also typically be used in spaces that are subject to additional risks such as theft or loss of devices. If the College fails to control and manage this process, then the College could be exposed to the risk of loss or theft of the device, information leakage, loss of information or tampering and reputational damage. The loss of personal data may lead to a fine or loss of financial or intellectual property.

2. Scope

The policy applies to all members of staff and students of the College and all other computer, network or information users (i.e. contractors, visitors, sponsored guests, any other third parties) authorised by the College.

It relates to their use of

- College managed laptops, tablets, smart mobile phones
- Personal mobile devices that are unmanaged by the College
- Mobile devices supplied by the College departments that are unmanaged by the College
- College rented mobile devices that are not managed by College
- Third party owned mobile devices
- Computing devices with in-built access points (e.g. WiFi NAS, mobile hotspots)

to access, store, transfer or transmit the College information.

3. Responsibilities

All: Each member of staff and student of the College and all other computer, network or information user authorised by the College, is individually responsible for the appropriate use of mobile working and security of the College data and will be responsible for any violations of this policy.

Head of Information Security: This role is responsible for ensuring that this policy is
enacted and ensure that the appropriate controls in place are formally identified and operating effectively.

**Information Security Team:** This role is responsible for overall development of this policy, and monitoring of its effectiveness.

**IT Services Staff in Departments, TSOs, IT Service Desk:** This role is responsible for applying technical controls defined in this policy.

4. **Policy:**

**Approved Usage of Mobile Working Technology**

4.1. Each member of staff and student of the College and all other computer, network or information user authorised by the College who uses mobile working must take all reasonable precautions to protect and control the mobile devices from unauthorised physical access, tampering, loss, theft and other threats.

**The College Managed Mobile Devices:**

4.2. The College may provide mobile devices to some of its members. The College managed mobile devices should be appropriately configured to ensure that they are as effectively managed as devices which remain within the office environment while they are being used in remote working. (See [Secure Build Policy](#), [Credentials Policy](#))

4.3. Appropriate encryption solution should be used for each College managed mobile device type (See [Secure Build Policy](#), for encryption of the cloud, 3rd party services storage refer to [Cloud/3rd Party Services Code of Practice](#))

4.4. For all College managed mobile devices, centralised Mobile Device Management (MDM) solution will be used for security controls and remote wiping functionality.

4.5. Non-members of the College must not make any use of the College managed mobile devices that contains sensitive data.

4.6. Users of the College managed mobile devices should be mindful of the risks of using open (unsecured) wireless networks. For securing sensitive College data during transmission, the College approved Virtual Private Network (VPN) solution should be used.

4.7. No unauthorised configuration changes (i.e. personal firewall settings, anti-virus configurations) may be made to the College managed mobile devices.

4.8. All of the College managed mobile devices must be returned to the College IT
prior to the recipient leaving the College.

**Personal Mobile Devices - Bring Your Own Device (BYOD)**

Personal mobile devices that are owned by individual members of the College; mobile devices supplied by the College departments that are unmanaged by the College; mobile devices that are initially managed by the College, but then became to unmanaged devices; and College rented mobile devices that are not managed by College are in the scope of this BYOD principles.

4.9. The College may allow its members to bring their own devices and access, process, store or transmit College information via personal mobile devices.

4.10. Users of personal mobile devices should understand and accept the guidelines (See Appendix) prior to connection of RHUL systems for accessing, processing or transmitting sensitive College data.

**Third Party Mobile Devices**

4.11. The College members should not use third party devices (i.e. devices in public libraries, hotels and cyber cafes) to access sensitive College information.

4.12. The security configurations of mobile devices of contractors and other third parties that have access to College data should at least be at the same level of College managed mobile devices. Contracts with 3rd parties should contain terms and conditions referencing College data access, storage, transfer, deletion and data protection policy (See [Cloud/3rd party Services Code of Practice](#)).

**Computing devices with in-built access points**

4.13. The College members should not use computing devices with in-built access points when accessing, processing, storing or transmitting sensitive College data (See [Wireless Access Policy](#)).

**Monitoring and Incident Reporting**

4.14. The Investigatory Powers Act (IPA) 2016, Regulation of Investigatory Powers Act (RIPA) 2000, the Lawful Business Practice Regulations (2000), and the Information Commissioner Code on Monitoring at Work (2003) provide the College the right to access all material, including email, held on College computing facilities where abuse is suspected or where there is a pressing academic or business need. Communications on or through the College’s computer systems may be monitored or recorded to secure effective system operations and for other lawful purposes. Note that the content of individual communications is not routinely monitored. However the College does reserve the right, within the law, to monitor in detail if there is some evidence of illegal or serious misuse of facilities, or if provision of the service may be
4.15 Each member of staff and student of the College and all other computer, network or information user authorised by the College should report if any mobile working device storing the College information is lost or stolen, or unauthorised disclosure or suspected unauthorised disclosure of the College information to IT Service Desk immediately via contact information in the Questions section of this policy.

5. Compliance

Each part of this policy states a requirement to audit and ensure compliance with the policy. A RACI model should be applied.

Responsible: Technical Service Owners/IT Service Desk/Departmental IT Staff
Accountable: Head of Information Services
Consulted: Head of Information Security
Informed: All Departmental IT, Information Security, IT staff

Compliance with this policy will be checked on the following schedule.

5.1 Annual IT compliance audits will be scheduled, checked and maintained.
5.2 Annual review of policy will be scheduled and reported.
5.3 Spot checks of policy compliance will be undertaken (minimum 1 per year), including review of reports and actions.
5.4 Annual device inventory audits for the College managed mobile device will be scheduled and reported.

6. Policy Exclusions:

There are no formal exclusions noticed for this policy. In case of any exception request, Information Security Exception Management process should be followed.

Questions:

If you have any questions on this policy or its execution, please contact:
IT Service Desk
01784 444321
itservicedesk@rhul.ac.uk
itservicedesk.rhul.ac.uk

Glossary:

**Encryption:** The process of converting information or data to an unrecognisable form, especially to prevent unauthorised access.

**Sensitive Data:** Data that must be protected from unauthorised access to safeguard the privacy of an individual and/or the security of the College. Sensitive data includes personal data (see Data Protection policy for details), financial data and data related to intellectual property. (See Data Management policy for definitions of data types).

**College Managed Mobile Devices:** Mobile devices that are centrally managed by IT Services. These devices are registered in Active Directory, are controlled by Group Policy, receive automated managed updates and are protected by the College anti-virus service.

**Related Documents:**
- IT Change control
- Incident Management
- Secure Build Policy
- Removable Media Policy
- Information Security Exception Management

**Acknowledgements**
- National Cyber Security Centre (NCSC)
- University of Leeds, University of Bristol
Appendix – Guidelines for Personal Mobile Device Usage

- The device must run a current version of its operating system. A current version is defined to be one for which security updates continue to be produced and made available to the device.
- An appropriate passcode/password must be set for all accounts that give access to the device (See Credentials Policy).
- A password protected screen saver/screen lock must be configured to “autolock” after a period of inactivity (no more than 10 minutes).
- Devices must remain up to date with security patches both for the device’s operating system and its applications.
- Devices which are at risk of malware infection must run anti-virus software and should have up-to-date signatures. The College will check such security controls upon remote access to the College Network via VPN.
- All devices which are no longer in use must be disposed of securely.
- Any use of personal devices by others must be controlled in such a way as to ensure that these others do not have access to sensitive College data.
- Consider configuring the device to “auto-wipe” to protect against brute force password attacks where this facility is available.
- Consider implementing remote lock/erase/locate features where these facilities are available.
- Do not undermine the security of the device (e.g. by “jail breaking” or “rooting” a smartphone).
- Do not leave mobile devices unattended where there is a risk of theft.
- Be aware of your surroundings and protect yourself against “shoulder surfing”.
- Be mindful of the risks of using open (unsecured) wireless networks. Consider configuring your device not to connect automatically to unknown networks.
- If a personally owned device needs to be repaired, take its backup, apply factory reset prior to repair service and after it’s repaired restore data from the backup (See device supplier guidelines for more information).
- Reduce the risk of inadvertently breaching the Data Protection Act by ensuring that all data subject to the Act which is stored on the device is removed before taking the device to a country outside of the European Economic Area or the listed countries (See https://www.gov.uk/data-protection/the-data-protection-act).
Document Control Sheet

Revision History

Date of this revision:    July 2017

Date of next revision:  July 2018

<table>
<thead>
<tr>
<th>Revision date</th>
<th>Summary of Changes</th>
<th>Changes marked</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2017</td>
<td>Initial Draft – 0.1</td>
<td>No</td>
</tr>
<tr>
<td>June 2017</td>
<td>Post initial workshop comments – 0.1</td>
<td>No</td>
</tr>
<tr>
<td>June 2017</td>
<td>Post TSO Workshop – 0.2</td>
<td>No</td>
</tr>
<tr>
<td>June 2017</td>
<td>Post ISSG Workshop – 0.3</td>
<td>No</td>
</tr>
</tbody>
</table>

Approvals

<table>
<thead>
<tr>
<th>Ratification by PRC</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval by Infrastructure and Security Sub-group</td>
<td>Yes</td>
</tr>
</tbody>
</table>