Removable Media Management Policy

Document Summary

<table>
<thead>
<tr>
<th>Document ID</th>
<th>Removable Media Management 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 removable media management rules which include the roles and responsibilities of users, approved removable media usage and approved usage of encryption.

The use of removable media to store or transfer information is an everyday requirement for the College, but storing or transferring sensitive College data should not be seen as business as usual. If the College fails to control and manage this process, then the College could be exposed to the risk of loss information, malware infection, information leakage, financial loss 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 staff and students of the College and all other computer, network or information users authorised by the College.

It relates to their use of any removable media that contains the College’s data or that are connected to the College network.

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 removable media and security of the College data and will be responsible for any violations to 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.

TSOs, IT Services Staff and IT Services in Departments: This role is responsible for applying technical controls defined in this policy.
4. Policy:

Removable Media:

Removable media is defined as devices or media that is readable and/or writable by the end user and are able to be moved from device to device.

The examples of removable media types are listed but not limited to, the following:

- External Hard Drives
- USB Memory Sticks (also known as flash memory devices, thumb devices)
- Media Card Readers
- Optical Disks (such as CDs, DVDs)
- MP3 Players
- Digital Cameras
- Mobile phone and tablet device storages

Approved Usage of Removable Media

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 removable media must take all reasonable precautions to protect and control the removable media from unauthorised physical access, tampering, loss, theft and other threats.

4.2. Sensitive information should be stored on removable media only when it’s encrypted and when it is required for the performance of assigned duties or when responding to legitimate requests for information with the minimum amount of data.

4.3. For research data sharing or professional services data sharing requirements, the College approved file sharing services should be used.

4.4. Unencrypted removable media devices must not be used to store or transfer any sensitive College information.

4.5. All types of removable media which store sensitive data should be encrypted to a minimum of Advanced Encryption Standard (AES) encryption method and 256 bit key. The College reserves the right to modify this requirement as new standards are published by US National Institute of Standards and Technology (NIST – www.nist.gov/publications).

4.6. Encryption can be done via tools that are mentioned in Standard Build Guidelines.

4.7. Automated on-access scanning of removable media for malware and viruses
should be configured on the College managed devices. In addition, appropriate technical controls should be applied to mitigate the risks. (See Mobile Working Policy)

4.8. In case of any removable media device which has College data is no longer in use, or have become damaged, must be securely wiped, disposed or physically destroyed based on the classification of the data held (See Data Management Policy).

4.9. All users are responsible for their actions regarding the use of removable media, this includes the use of removable media provided by third party.

4.10. If there are any third party contractual terms relating to specific data that exceed the College policies, they should be respected and enacted.

4.11. In some specific cases, the College reserves the right to restrict removable media usage in specific environments.

4.12. When responding to legitimate business or legal requests, the College encourages the use of pin-protected removable media devices for transferring sensitive data that can be requested from IT Services.

**Monitoring and Incident Reporting**

4.13. The Investigatory Powers Act (IPA) 2016, The Regulation of Investigatory Powers (RIP) Act 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 compromised (See IT Regulations and Legal Information - [https://www.royalholloway.ac.uk/it/tos/regulations.aspx](https://www.royalholloway.ac.uk/it/tos/regulations.aspx)).

4.14. Each member of staff and student of the College and all other computer, network or information user authorised by the College should report the loss or theft of any removable media storing the College sensitive information to IT Service Desk immediately.

4.15 Each member staff and student of the College and all other computer, network or information user authorised by the College should report if an unknown
removable media device is found unattended to the IT Service Desk. Current legal advice suggests that users should not touch the device.

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.

6. Policy Exclusions:

6.1. This policy doesn't cover paper files but College states that paper files with sensitive College data (printed by a College printer or any printer e.g. at home or directly by a 3rd party) have the risk impact of financial loss and reputational damage by means of loss, theft, etc. and require the same level of security with removable media devices storing sensitive data.

In case of any exception request to this policy, 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
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).

Related Documents:

- IT Change control
- Incident Management
- Mobile Working Policy
- Standard Build Guidelines (Guidelines are being prepared)
- Information Security Exception Management

Acknowledgements

- National Cyber Security Centre (NCSC)
### 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 – 0.2</td>
<td>No</td>
</tr>
<tr>
<td>June 2017</td>
<td>Post TSO Workshop – 0.3</td>
<td>No</td>
</tr>
<tr>
<td>June 2017</td>
<td>Post ISSG Workshop – 0.4</td>
<td>No</td>
</tr>
</tbody>
</table>

**Approvals**

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