GDPR considerations when working away from the office

Whilst remote working has its benefits, it also has exacerbated risks. To ensure protection of personal data for which the College is responsible, all employees working remotely must be vigilant in terms of where sensitive data could potentially be lost or exploited through remote working vulnerabilities.

The purpose of this guidance is to highlight the risks of remote working and to establish the standards and working practices required of remote workers by the College.

Colleagues should ensure they have completed the GDPR training available on Moodle.

1. **Avoid using public computers and public Wi-Fi for work**

   Ensure you refer to the guidance from IT about how to connect securely to College services from home.

2. **Cyber Security**

   You should refer to the guidance on the staff intranet pages about how to keep your devices safe when working at home. This includes setting up Multi-Factor Authentication.

3. **Physical Security**

   Do not download work documents to your personal computer or laptop hard drive. Loss or theft of an electronic device used for work purposes will likely constitute a data breach and should be reported to the Data Protection Officer at dataprotection@rhul.ac.uk.

   If you are working outside of the home, be aware of shoulder surfers, who may be looking at confidential information that is displayed on your screen.

4. **Removable Media (USB sticks)**

   With access to all College drives available via the VPN there should be no need for anyone to take home data on a USB stick or other removable media device. These are easily mislaid and therefore represent a high risk of data being lost, particularly if unencrypted.

   There should also be no need for anyone to send work documents to their personal email addresses. Personal email accounts are not secure.

5. **Paper documents**

   Where possible, remote workers are encouraged to go paperless, only using their devices to access all documents, unless it's strictly necessary to print them.

   Paper documents are un-trackable and impossible to protect. Therefore, if the use of paper is unavoidable, then it should be stored as securely as possible within the home and kept out of sight of anyone except authorised employees. Following its use, all documentation must be destroyed in line with the College's document retention policies. This may involve employees bringing in unwanted documents when they come into the office for confidential waste disposal.

   Under no circumstances should College data be thrown away with normal household waste or recycling.