## Staff Email Usage Policy

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Executive Board is asked to approve this policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>The policy sets out responsibilities for staff in terms of their use of email, as well as expectations for how their accounts will be managed by College.</td>
</tr>
<tr>
<td>Strategic context</td>
<td>Compliance with legal obligations; security of IT facilities</td>
</tr>
<tr>
<td>Strategic risks</td>
<td>Without approval, College’s ability to respond to certain legislative requirements is hindered.</td>
</tr>
<tr>
<td>Resource implications</td>
<td>None</td>
</tr>
<tr>
<td>Previous review</td>
<td>Executive Board – September 2019</td>
</tr>
<tr>
<td>OfS reportable event</td>
<td>No</td>
</tr>
<tr>
<td>Next steps</td>
<td>Publish and circulate policy</td>
</tr>
<tr>
<td>Date of introduction</td>
<td>Immediate</td>
</tr>
<tr>
<td>Author</td>
<td>Christine Cartwright, Compliance and Data Protection Manager</td>
</tr>
<tr>
<td>Senior Responsible Officer</td>
<td>Mike Johnson, Chief Information Officer</td>
</tr>
<tr>
<td>Date of writing</td>
<td>22 April 2020</td>
</tr>
</tbody>
</table>
Royal Holloway, University of London

Staff Email Usage Policy

Scope

This policy is to make staff aware of their obligation to use email responsibly, professionally, ethically and lawfully and to make them aware of the rights and activities of the College regarding the monitoring of its use.

Staff should be aware that improper use of email may have adverse consequences for themselves or the College, such as unauthorised disclosure of confidential and proprietary information, reputational damage to individuals or the College and potential breaches of the law. Examples of potential breaches of the law could include, but are not limited to, posting of defamatory or libellous material, divulging personal data and infringement of third-party intellectual property rights.

Guidance on acceptable use and content of emails is provided at Appendix 1 of this policy.

Privacy

Emails sent on the College email system form part of the official records of the College; they are not private property and may be disclosed under the Freedom of Information Act 2000 and Data Protection Act 2018, as part of legal proceedings, and as part of disciplinary proceedings. Members of staff are responsible for all actions relating to their email account and should therefore make every effort to ensure no other person has unauthorised access to their account.

The College reserves the right to remotely search the contents of any email account without the knowledge or permission of the account holder in order to comply with legal obligations.

Security

Users of College IT facilities must take all reasonable steps to prevent the receipt and transmission by email of malicious software e.g. computer viruses.

In particular, users:
- must not transmit by email any file attachments which they know to be infected with a virus;
- must ensure that an effective anti-virus system is operating on any computer which they use to access College IT facilities;
- must alert the IT Service Desk if they receive any malicious software notifications from the anti-virus solution.
- must not open email file attachments which are received from unsolicited or untrusted sources.
- must not click on links within unsolicited or untrusted e-mails.

Staff should forward any email they suspect to be compromised in any way to the IT Service Desk or report it using the tools in Outlook.

Staff must alert the Cyber Security team via the IT Service Desk of any suspicious e-mails which they may have interacted with.

Staff who receive e-mail containing suspicious attachments must not share the attachment with colleagues in an attempt to open the attachment.

All staff must undertake regular IT security training in particular with reference to phishing emails.
Monitoring

Where the College has reasonable grounds to suspect misuse of email in terms of either the scale of use, or the content or nature of messages, it reserves the right to intercept (if necessary) and to monitor the relevant accounts including but not limited to the destination, source and content of email. The use of email (for either personal or business purposes) to send or forward messages or attachments which are in any way defamatory, obscene, or otherwise inappropriate will be treated as misconduct under the appropriate disciplinary procedure.

We reserve the right to retrieve the contents of email messages as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

- To monitor whether use of the email system or the internet is legitimate and in accordance with this policy.
- To find lost messages or to retrieve messages lost due to computer failure.
- To assist in the investigation of alleged wrongdoing.
- To comply with any legal obligation.
- To remotely erase emails which were sent in error.
- To defend Royal Holloway’s information assets from the actions of internal and external threat actors.

Breach of this policy may be dealt with under the relevant disciplinary procedure and in, in serious cases, may be treated as gross misconduct leading to summary dismissal.

Personal Use

You are advised to use personal email accounts for personal communication where possible. We permit the incidental use of our systems to send personal email, subject to certain conditions. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

Personal uses must meet the following conditions:

- It must be minimal and take place substantially outside of normal working hours (that is, during your lunch break and before or after work)
- It must not affect your work or interfere with the business.
- It must comply with our policies including this policy, the Equal Opportunities Policy, Anti-harassment and Bullying Policy, Data Protection Policy, Disciplinary Rules and Disciplinary Procedure.

Expiry of Accounts

Access to all IT systems and email accounts will normally be withdrawn at the end of your last day of service at Royal Holloway.

Further Information

If anyone considered that this policy has not been followed they should raise the matter with IT Services.

<table>
<thead>
<tr>
<th>Policy Owner</th>
<th>Chief Information Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approving Body</td>
<td>Executive Board</td>
</tr>
<tr>
<td>Version number</td>
<td>1</td>
</tr>
</tbody>
</table>
| Related policies, procedures and guidelines | Disciplinary policy  
|                    | Personal Harassment Code of Practice |
| Reviewed by        | Cyber Security             |
| Approved on:       |                           |
| Review Deadline    | September 2022            |
Appendix 1

Standards of Use

All email is intrinsically insecure unless it is encrypted, therefore when sending emails internally and externally you must comply with College policy, in particular:

- Always use care in addressing email messages to make sure that the messages are not inadvertently sent to the wrong person or sent outside the company.

- Exercise caution in transmitting confidential information.

- When sending attachments that contain sensitive personal data, you should apply password protection and send the password separately.

- Where the content of the email is of a confidential or sensitive nature, you should:
  o Use discretion when considering transmission by email. Consider whether email is an appropriate medium.
  o If a matter is particularly complex or confidential, consider whether a phone call or meeting would be the best means to communicate.
  o Stipulate the content of the email is of a confidential nature. This can be done in the options (personal), subject line and/or in the body of the email.

- Your emails should be courteous, professional and business like. They may be read by someone other than the person to whom you send them as they may have to be disclosed to third parties following a request made under the Freedom of Information Act 2000 or subject access request made under the Data Protection Act 2018. They may also be disclosed in connection with litigation.

- You should only copy in those people who genuinely need to read the email, as otherwise it contributes to potential breach of confidence as well as system congestion. You are not absolving yourself of responsibility by copying them in.

- Do not send messages from another person’s email address unless authorised to do so.

- Staff should use their Royal Holloway accounts for all emails discussing College business or where they are acting in their capacity as employees of the Royal Holloway, University of London.

- Staff should not use their Royal Holloway email address to register for third party services which are not related to their work e.g. online gaming or shopping.

- Staff should not auto-forward emails received by their Royal Holloway account to any third-party provider, nor conduct College business through third party providers, as to do so places the content of those emails, and potentially sensitive College business, at risk.

Standards of Content

Email should not be used:
- for the creation or transmission (other than for properly documented, supervised and lawful research purposes) of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material
- for the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety
- for the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others
• for the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.

• for the creation or transmission of defamatory material

• for the creation or transmission of material that includes false claims of a deceptive nature

• for activities that violate the privacy of other users

• for criticising individuals, including copy distribution to other individuals

• for the creation or transmission of anonymous messages, i.e. without clear identification of the sender

• for the creation or transmission of material which brings the College into disrepute.