UNIVERSITY OF PORTSMOUTH

STAFF EMAIL POLICY

May 2024

Contents

Document title		
Staff Email Policy		
Document author and department		
Sarah Arnold, University Records Manager, Corporate Governance		
Approving body		
Claire Dunning, Executive Director of Corporate Governance		
Date of approval		
8th May 2024		
Review date		
May 2027		
Edition no.		
7		
ID Code		
70		
Date of effect		
13th May 2024		
EITHER For public access online (internet)? *Tick as appropriate*		**YES**
For public access on request copy to be mailed *Tick as appropriate*		**YES**
OR For staff access only (intranet)? *Tick as appropriate*		
Password protected *Tick as appropriate*	**NO**	
External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk If you need this document in an alternative format, please email corporate.communications@port.ac.uk		

The latest version of this document is always to be found at:

http://policies.docstore.port.ac.uk/policy-070.pdf

Summary

What is this document about?

The Staff Email Policy sets out the conditions under which the University's email system will be used, and the principles for managing messages created or received as part of the University's business. Staff at the main Portsmouth campus are currently using Google Workspace for Education. Staff at UoP London campus are using Microsoft 365. For the avoidance of doubt, where this policy references Google or Microsoft, staff should refer to the information for the platform they are currently on at the time of reading.

Who is this for?

It applies to all staff and other authorised account holders (i.e. those with an @port.ac.uk email address) including PhD students and governors.

The University proactively raises awareness of this policy as a means of ensuring it will be followed by all staff. Staff members are informed of the existence of this policy and the need to manage their emails effectively at the staff induction conference, via the Information Governance eLearning package which is part of the University's core training, via awareness campaigns, and via an annual reminder (Staff Essentials news article).

The use of email by students and alumni (@myport.ac.uk email addresses) is covered by the Student Email Policy which can be found in the policy section of the University website.

How does the University check this is followed?

Library and Information Services (LIS) carry out monitoring to scan for phishing emails and as part of Data Loss Prevention to prevent sensitive information being inappropriately sent outside of the organisation. Reactive monitoring may be carried out in accordance with section 2.7 of this Policy.

Who can you contact if you have any queries about this document?

Any questions about this Policy should be directed to the University Records Manager.

Executive summary

The key elements of the Staff Email Policy are:

1. Email facilities are provided to support learning, teaching, research, administration and approved business activities of the University. All @port.ac.uk email addresses, associated accounts (including @portsmouth.ac.uk addresses) and emails are the property of the University.
2. Emails are subject to the same laws and policies that apply to other forms of communication, and therefore must be composed with the same degree of care as would be used for formal letters.
3. All University email correspondence must be conducted using the University's email facility.
4. Communication undertaken on behalf of the University is subject to the University's Dignity and Respect policy, which promotes the principles of respect and dignity in all correspondence.
5. All emails are subject to Data Protection and Freedom of Information legislation, and may be legally admissible. This also applies to all instant messaging platforms used for work purposes, including but not limited to Chat messages. Statements must not be made that could expose the University to legal liability or damage its reputation.
6. In order to present a consistent and professional image to those with whom the University corresponds, staff are expected to adhere to corporate guidelines when creating their email signature.
7. In cases of planned absence, staff must set up an out-of-office email message giving alternative contact details to ensure that enquiries can be answered promptly and that Freedom of Information requests can be answered within legally prescribed timescales (see section 3.6.1 for a suggested form of words).
8. Where appropriate to their role, staff may give a colleague delegated access to their email account, so that messages can be checked in cases of staff absence/illness.
9. Emails are records of the University's actions and decisions, and must be managed as efficiently as paper and other electronic records. It is the responsibility of all staff to ensure that messages with continuing value are saved into the appropriate corporate system.
10. Users must regularly review their emails to ensure that those that have served their purpose are deleted from the system. For more info, please see Records Management Factsheet 04 – Managing Emails and Other Modern Media
11. Staff are not permitted personal use of university systems.
12. Any misuse of the system may cause the instigation of formal disciplinary procedures and the police authorities may be notified (see the whole of section 2 for more details, but primarily 2.2 and 2.7).
13. When members of staff leave the University or move to another part of the University, it is their responsibility to transfer to appropriate colleagues or systems any messages that need to be retained. Accounts of staff leavers will be deleted 6 months after their leave date, in accordance with the Staff Access to Facilities and Staff Leavers procedure.
14. Staff should ensure that their electronic work diaries are held within University-approved systems and kept up-to-date, so that colleagues can easily confirm their availability when booking appointments and arranging meetings.

Policy

1. Introduction

The purpose of this Policy is to set out the conditions under which the University's email system may be used, and the principles for managing messages created or received as part of the University's business. It applies to all staff and other authorised account holders (i.e. those with @port.ac.uk email addresses, including PGR students). The use of email by students (i.e. @myport.ac.uk email addresses) is covered by the Student Email Policy which can be found in the policy section of the University website.

1.1. Responsibilities

Responsibility for reviewing and updating this Policy lies with the University Records Manager, authorised by the Executive Director of Corporate Governance. Line managers have a responsibility to ensure that their staff are aware of the Policy, and all users are expected to comply with its requirements.

1.2. Ownership

The University provides all staff with either Google Workspace for Education accounts or Microsoft 365 accounts for the duration of their employment. After this time the email address and all other related services will be retired from use. The data will then be deleted 6 months after the account is retired, in accordance with the Staff Access to Facilities and Leavers Procedure, which can be found in the policy section of the University website.

All @port.ac.uk email addresses, associated accounts, work-related emails and instant messages are the property of the University. Ownership allows the University the right to access/monitor emails and, if necessary, their content (see paragraph 2.7 below for further information).

1.3. Data Protection

The University acts as the domain administrator for Google and Microsoft facilities and administers all email accounts in accordance with its Data Protection Policy (available in the policy section of the University website).

For information on how Google and Microsoft manage personal data, please refer to their privacy policies, linked from section 1.5 below.

1.4. Legislation

Emails and instant messages are subject to the same laws that apply to other forms of communication, including those covering defamation, harassment, copyright and data protection. Users should ensure that they read the Appendix to this Policy, which briefly describes the main pieces of legislation that have a bearing on the use and transmission of emails and instant messages and, if uncertain, seek advice.

1.5. Related policies and documentation

This Policy should be read in conjunction with the following policies and guidelines. This list is not exhaustive.

1.5.1. University policies

All available in the policy section of the University website.

- Dignity and Respect Policy
- Data Protection Policy
- Freedom of Information Policies
- Information Security Policy
- Records Management Policy
- ICT Acceptable Use Policy

1.5.2. Factsheets and Advisories

- Records Management Factsheet 04 – Managing Emails and Other Modern Media (intranet link, VPN use required)
- Information Security Advisories

1.5.3. Google policies

- Google Workspace for Education Acceptable Use Policy
- Google Privacy Policy

1.5.4. Microsoft policies

The Microsoft Product Terms, covering:

- Microsoft Acceptable Use Policy
- Microsoft Privacy Policy

1.5.5. Third party policies

- JANET Acceptable Use Policy

2. Conditions of use

Email facilities are provided to support learning, teaching, research, administration and approved business activities of the University.

Any member of staff, who is also enrolled as a student, must ensure that they use their staff account alone to conduct University business. Likewise, any emails sent or received in their capacity as a student, must be sent from/received into their student account.

Staff should always use their University email address to conduct University business. This is to ensure that the University has a record of all business correspondence and to enable the University to back up emails for business continuity purposes. University email accounts are web-based and can be accessed from any location with internet access. In addition, provision has been made for offline access to emails, when necessary.

Emails and instant messages are disclosable under various laws and must be composed using the same degree of care as would be used for a formal letter. They are potentially disclosable to external parties and statements must not be made that could expose the University to liability or damage its reputation.

All communication undertaken on behalf of the University is subject to the University's Dignity and Respect policy (available in the policy section of the University website).

Staff should ensure that their electronic work diaries are held within Google Workspace Calendar or Microsoft Outlook Calendar (as appropriate) and kept up-to-date, so that colleagues can easily confirm their availability when booking appointments and arranging meetings.

Account holders must comply with the JANET Acceptable Use Policy, the Google Workspace for Education Acceptable Use Policy and the Microsoft Acceptable Use Policy (see 1.5 above for links).

2.1. Security

Users are responsible for the security of their mailboxes. The use of multifactor authentication (two-step verification) with University Google and Microsoft accounts is mandatory.

Although emails are automatically scanned for virus content and spam, account holders are expected to take reasonable measures to prevent the introduction and transmission of computer viruses. These include:

- not opening attachments received from unsolicited or untrusted sources;
- not transmitting attachments known to be infected with a virus;
- ensuring that antivirus/anti-spyware software is installed and maintained on any personal computer used to gain access to the University's IT facilities.

The LIS Service Desk should be informed immediately, if a suspected virus is received or a user becomes aware that someone has gained unauthorised access to their account, or potentially obtained their personal details (e.g. disclosed via a phishing attack).

Staff must lock their work stations (windows key+L on a Windows PC) when away from their desk, even for short periods. Computers which cannot be locked must not be left unattended whilst logged-on.

Email passwords are synchronised with the University standard network passwords. Users should use strong passwords and must never disclose their passwords to others. If it is necessary to provide another user with access, delegation should be employed (see section 2.4), which enables authorised access without the sharing of passwords. Advice on creating a strong password can be found on the Information Security Advisories page.

The unauthorised interception of, or access to, the messages of others is illegal and a breach of this policy. Access may be authorised via delegation (see section 2.4 below), or as part of a formal monitoring process (see section 2.7 below).

2.2. Prohibited use

The University email facilities must not be used for:

- the creation, transmission or storage of text, images and other material that is offensive, obscene, indecent, discriminatory, harassing, libellous or defamatory;

- the transmission of material that infringes the intellectual property rights of another person, including copyright;
- the creation or transmission of material that brings the University into disrepute;
- any activity that is illegal, including (without limitation) the creation or transmission of material that is illegal;
- the incitement of violence;
- unauthorised transmission to a third party of confidential material concerning the activities of the University;
- the transmission of unsolicited commercial or advertising material, chain letters or other junk mail;
- activities that corrupt or destroy other users' data or disrupt the work of others;
- activities that violate the privacy of others or unfairly criticise or misrepresent others;
- personal use.

This list is not exhaustive. Use of this type may result in the suspension of a user's email facilities for as long as necessary to conduct an investigation. The instigation of formal action under the staff disciplinary procedures may follow and, in certain circumstances, legal action may be taken.

Some countries restrict access to various websites and/or Internet-based services. If you are travelling abroad and think you may need to use your University email account and related services, please consult this webpage for more information before you travel.

2.3. Personal use

Personal use of the University's IT systems is not permitted.

Staff should be aware that information disclosure requirements may also apply to work related emails sent from a personal email account. For this reason, personal email accounts should not be used for sending or receiving work related emails.

2.4. Delegated access

Where appropriate to the role (e.g. staff with PAs/EAs, or staff in job share roles), staff may give delegated access to their account, so that business emails can continue to be answered in cases of unexpected or prolonged absence.

Unless otherwise agreed between the user and their delegated colleague, access should only be used in times of absence or emergency. Anyone who is granted access to another user's account must respect the confidentiality of that account.

2.5. All-staff emails

The all-staff email facility is a useful means of conveying information and, when necessary, important and urgent messages to all staff of the University. It is, however, important that the facility is used appropriately and not over used. All staff have a duty to read all-staff emails.

Weekly all-staff newsletters are distributed on a Monday afternoon and contain a selection of news articles from the week. New submissions of appropriate content for UoP news articles can be made via the Service Desk Form, or email the Staff News mailbox.

At other times, all-staff emails can be sent by:

- Members of UEB
- Chief Information Officer (or Service Desk)

- Internal Communications Team
- Selected individuals with a demonstrable need to send all-staff emails, as approved by the Internal Communications Manager

The Internal Communications Manager will be responsible for ensuring that posting permissions to the All Staff Email group are kept up to date.

These all-staff emails are for the timely dissemination of information considered important to all staff and may encompass the following categories:

- Information relevant to the security, operation or suspension of IT systems
- Health and safety matters
- Access issues where buildings may be affected
- Strategic and operational information from UEB
- Governance and legal compliance matters
- Critical incidents

In case of doubt, please refer to the Internal Communications Manager (Marketing and Communications) for a decision on whether the sending of an all-staff email is appropriate.

2.6. Authorised Research

Research is part of the core business of the University. From time to time staff will be contacted on their University email address for the purpose of voluntary recruitment into studies that have received a favourable opinion from a research ethics committee. Such contact will only come from within the University of Portsmouth.

2.7. Monitoring

The University will carry out monitoring to guard against cyber-attacks or mis-use. All content stored within the Google or Microsoft environments may be monitored for security purposes. This monitoring may be carried out by the University, or by a third party on behalf of the University. In the event of an identified cyber-attack, human intervention and access to emails may be required.

The University, as the domain administrator for facilities provided by Google or Microsoft, may use analytical tools to monitor the University's use of these platforms and have access to information held in any University account. The University reserves the right to access this information in the following circumstances:

- in connection with a criminal investigation;
- in connection with a properly authorised investigation in relation to breaches or alleged breaches of the University’s rules on use (including but not limited to whistleblowing, fraud and bribery);
- to meet legal or statutory requirements;
- in a situation (such as prolonged staff absence) where access is required to enable the University’s business to continue;
- in an emergency situation, including as a response to a potential cyber incident.

This list is not exhaustive. Any University monitoring that takes place will be conducted by LIS staff (or authorised third parties); will be authorised by the Executive Director of Corporate Governance; and will be in line with the requirements of the Information Commissioner's Office guidance on monitoring workers. Where there is evidence of a breach of University policy or an offence, it will be investigated in accordance with the University's disciplinary procedures. The University reserves the right to require that encryption keys, where used, are made available, so that it can gain access to relevant emails as part of an investigation.

Additionally, Google and Microsoft will conduct their own monitoring for security purposes. Please refer to their respective Privacy policies (see 1.5 above) for more information.

2.8. Confidentiality

Email, like any other form of communication, is not completely secure and its confidentiality cannot be guaranteed: messages can be intercepted by third parties, wrongly addressed, forwarded accidentally and forwarded by recipients to third parties. Before transmitting information of a confidential nature, users should assess whether it is appropriate to transmit the data in the email itself, or whether it should be in a document attached to/linked from the email. If documents containing sensitive information are sent from the University's network to external addresses, staff must encrypt them. (For guidance on how to encrypt documents please contact the IS Service Desk on extension 7777 or via Hornbill. Annex C of the Data Protection Policy, available in the policy section of the University website, provides guidance on classifying the sensitivity of data.)

Before forwarding messages – whether externally or internally – staff should consider whether the authors of the messages would expect or be willing for this to happen. Staff should also consider whether the transmission of the information would breach the privacy of an individual or infringe copyright. In cases where it is necessary to send a message to a number of individuals – some (or all) of whom do not work for the University – care must be taken to prevent the recipients' email addresses from being disclosed unlawfully: the 'BCC' facility should be used to ensure that the addresses of the recipients cannot be viewed by each member of a distribution list.

3. Management of emails

Emails are records of the University's actions and decisions, and must be managed as efficiently, and in the same way, as paper and other electronic records. There should be consistent, coherent controls in place to meet business and accountability needs, as well as to ensure legal compliance.

Messages must be checked regularly, prioritised and answered as promptly as possible. They should also be stored logically to ensure that information can be managed effectively and readily retrieved in response to enquiries (such as Data Protection and Freedom of Information requests). Staff are encouraged to tag emails with metadata to aid the management of current mail and retrieval of archived mail.

3.1. Training and Guidance

Training on the use of Google Mail and Calendar is available from IT Training (Short Sessions).

Guidance on the management of emails can be found on the University's Records Management intranet pages (VPN use required to follow this link).

For further guidance on managing emails in Google, please see the Google Help pages.

For further guidance on managing emails in Microsoft, please see the Microsoft Support site.

3.2. Email Signatures

In order to present a consistent and professional image to those with whom the University corresponds, staff are expected to adhere to corporate guidelines when creating their email signature. Details of how to construct an email signature which conforms to the required layout and formatting can be found here.

The logos used in the signature (e.g. external rankings and accolades) will be reviewed regularly and, where appropriate, updated to reflect those that most enhance our reputation. Staff will be informed when the logos to be used in the approved email signature change.

3.3. Retention and Deletion

It is the responsibility of all staff to ensure that messages with continuing value are saved. Emails cannot be treated as a single series with a single retention period: the length of their retention must be determined by their subject matter or business purpose, as is the case with any other electronic or paper record.

Retention decisions should take into account business/operational needs, legal and regulatory requirements, accountability and transparency expectations. Messages relating to complaints, appeals, disputes and grievances should be retained as long as there is a need to preserve an audit trail or a risk of legal action arising. The University reserves the right to apply automated retention and deletion, in line with policies, to our services.

The risk implications of deleting messages must be considered, as well as the obligation to comply with the Data Protection Principle ‘Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed’. All emails that are retained will be subject to Data Protection and Freedom of Information legislation, and may be legally admissible.

Where the University is party to a criminal investigation or a civil legal dispute, it is obliged to retain all relevant evidence. In such circumstances, staff should seek advice from the University Solicitor as to compliance requirements if unsure.

Users are obliged to review their emails (both their inbox and their archived mail) on a regular basis to ensure that those that have served their purpose are deleted. Messages that are no longer needed should be moved to the Bin. Users should be aware that all items placed in the Bin will be automatically deleted after thirty days and cannot be recovered. Whilst information is held in the Bin, it will be considered still accessible and may therefore have to be disclosed (in the period before erasure) in response to requests made under the Freedom of Information or Data Protection legislation.

3.4. Shared email accounts

In departments where several staff are responsible for the same area of work and require access to the same emails, it may be helpful to use a shared (generic) email account. Sharing access to a single account should make it easier to answer messages promptly and manage them effectively when individual members of the team are away. Using a shared email account should also simplify the process of sorting accounts when staff leave: if team members keep the majority of their emails in a shared mailbox, less time should be required for reviewing individual accounts when staff leave the University or transfer to another department (see section 3.7).

Each shared email account requires a primary contact who is responsible for the overall management of the mailbox, ensuring there are effective procedures in place for controlling incoming and outgoing messages. Access to shared email accounts is granted by the IS Service Desk, using delegation.

If shared email accounts are decommissioned (e.g. due to organisational changes) departments should ensure either that any email sent to the decommissioned email address is forwarded to the appropriate live mailbox, or that an out-of-office response is set up to inform enquirers that the mailbox is no longer live and give them alternative options for submitting their enquiry to the correct department.

3.5. Instant messages

Instant messaging in Google saved in Google Workspace for Education, if one or more of the people involved in the conversation have the history set to "on".

Instant messaging in Teams are also saved and this cannot be turned off. The University will be setting default rules around the retention of chat content in Microsoft.

This means that instant messages could be disclosed to external parties in response to requests made under the Freedom of Information or Data Protection legislation. Statements must not be made that could expose the University to legal liability or damage its reputation. Other instant messaging platforms (such as MS Teams Chat) may also be in use in some areas of the business and are subject to the same legal disclosure and required standards of use.

3.6. Absence from the University

3.6.1. Planned absence

In cases of planned absence, staff must set up an out-of-office message giving alternative contact details to ensure that enquiries (including those relating to Data Protection and Freedom of Information) can be answered promptly.

A suggested form of words for out of office messages is: "I am away from the University until [enter date here]. If your email is urgent, or a request made under the Freedom of Information Act, please contact my colleague [enter colleague's name and email address here] in the first instance".

3.6.2. Illness or other unforeseen circumstances

In cases of illness or other unforeseen circumstances, where it is not possible to make any preparations for being away from the office, staff may already have nominated a colleague to have delegated access to their account, so that emails may be dealt with in their absence (please see section 2.4).

If the staff member has failed to nominate a colleague for delegated access, the member of staff's line manager should take the following actions:

- Set up an automatic reply. To do this, the line manager should log a job with the IS Service Desk, requesting that an auto-reply is added to the relevant staff account and supplying the exact text for the reply.
- Set up an auto-forwarding facility, if necessary. To request auto-forwarding, the line manager should similarly log a request with the IS Service Desk.
- Ensure emails received in the intervening period are dealt with, as necessary. If the line manager needs to gain access to the account to check whether there are business emails requiring attention, they should follow the procedures specified by the information security advisory on third party access procedures.

3.7. Leaving a department or the University

When members of staff leave one department to transfer to another, or leave the University, it is their responsibility to delete all messages with no continuing value and to transfer to appropriate colleagues or into relevant corporate systems any messages that need to be retained.

Users should be aware that, once they have left the University, they will no longer have access to their @port.ac.uk email account, as this is the property of the University. It is therefore highly inadvisable to link any personal devices or personal logins to your @port.ac.uk account in a way which will would prohibit your use of that personal device or login when your account is closed.

For further details about the procedures to be followed when members of staff leave, please see 'Staff Access to University Facilities and Leavers' Procedures' (available in the policy section of the University website).

3.8. Further information

For further information about Google Mail accounts, please contact the IS Service Desk:

- Hornbill
- Telephone: 023 9284 7777
- IS MyPort Article Hub

IT Training (Short Sessions)

For guidance on using Google Mail, please visit the Google Help pages.

For guidance on using Outlook Mail, please visit the Microsoft Support site.

University of Portsmouth
Corporate Governance
Mercantile House
Hampshire Terrace
Portsmouth PO1 2EG
United Kingdom

T: +44 (0)23 9284 3141
E: corporate-governance@port.ac.uk
W: www.port.ac.uk