Staff Email Policy (Google Mail)

September 2015

University of Portsmouth

Document title			
Staff Email Policy (Google Mail) September 2015			
Document author and department			**Responsible person and department**
Sarah Arnold, University Records Manager, Corporate Governance			Adrian Parry, Director of Corporate Governance
Approving body			**Date of approval**
Adrian Parry			August 2015
Review date	**Edition no.**	**ID Code**	**Date of effect**
June 2018	4	70	1 September 2015

EITHER **For public access online (internet)?** *Tick as appropriate*	**OR** **For staff access only (intranet)?** *Tick as appropriate*
Yes ✓	**Yes**
For public access on request copy to be mailed *Tick as appropriate*	**Password protected** *Tick as appropriate*
Yes ✓ **No**	**Yes** **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:

www.port.ac.uk/accesstoinformation/policies/informationservices/filetodownload,64582,en.pdf

Contents

Staff Email Policy (Google Mail)

Summary

What is this Policy about?

The Staff Email Policy sets out the conditions under which the University's email system – Google Mail – may be used, and the principles for managing messages created or received as part of the University's business.

Who is this Policy for?

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

The use of Google Mail by students is covered by the Student Email Policy which can be found at **www.port.ac.uk/accesstoinformation/policies**.

How does the University check this Policy is followed?

Given the volume and nature of email accounts, proactive monitoring is neither practicable nor desirable. Reactive monitoring may be carried out in accordance with section 2.6 of this Policy.

However, staff members are informed of 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 email.

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

Any questions about this Policy should be directed to the University Records Manager at **recordsmanagement@port.ac.uk**.

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 and work-related 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 work-related email correspondence must be conducted using the University's Google Apps.

4. Communication undertaken on behalf of the University is subject to the University's Anti-Bullying and Harassment Policy, which espouses the principles of respect and dignity in all correspondence.

5. All work-related emails and instant messages are subject to Data Protection and Freedom of Information legislation, and may be legally admissible. 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 message giving alternative contact details to ensure enquiries can be answered promptly and that Freedom of Information requests can be answered within legally proscribed timescales.

8. Staff should give a colleague delegated access to their email account, so that messages can be checked in cases of staff absence/illness.

9. Work-related 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.

10. Users must regularly review their emails to ensure that those that have served their purpose are deleted from the system.

11. Users are permitted a reasonable level of personal use.

12. Any misuse of the system may cause the instigation of formal disciplinary procedures and, in severe cases, the police authorities may be notified.

13. When members of staff leave the University, it is their responsibility to delete all messages with no continuing value including personal emails and to transfer to appropriate colleagues or systems any messages that need to be retained.

14. Staff should ensure that their electronic work diaries are held within Google Apps Calendar and kept up-to-date, so that colleagues can easily confirm their availability when booking appointments and arranging meetings.

1. Introduction

The purpose of this Policy is to set out the conditions under which the University's email system – Google Mail – 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. The use of Google Apps Mail by students is covered by the Student Email Policy which can be found at **www.port.ac.uk/accesstoinformation/policies**.

1.1 Responsibilities

Responsibility for reviewing and updating this Policy lies with the 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

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 2.6 below for further information).

1.3 Personal data

Google Mail and its related applications (e.g. Google Drive, Google Calendar, Google Hangout) are hosted offsite. Google handles all personal data in line with its Privacy Policy (**www.google.co.uk/policies/privacy/**) and adheres to the European Union Safe Harbor Framework (**www.export.gov/safeharbor**). The University is signed up to the JANET contract with Google, which addresses the requirements of Data Protection legislation.

The University acts as the domain administrator for Google facilities and administers all email accounts in accordance with its Data Protection Policy (available at **www.port.ac.uk/accesstoinformation/policies**). For further details, please see **www.google.co.uk/policies/privacy/**.

1.4 Legislation

Please see the Appendix for a brief description of the main pieces of legislation that have a bearing on the use and transmission of emails.

1.5 Related policies and documentation

This Policy should be read in conjunction with the following policies and guidelines.

1.5.1 University policies

All available at **www.port.ac.uk/accesstoinformation/policies**.

- Anti-Bullying and Harassment Policy
- Data Protection Policy
- Freedom of Information Policies
- Information Security Policy
- Records Management Policy
- Staff Communications Policy
- Student Communications Policy
- Guidelines for Dealing with Email and Post in Cases of Staff Absence

1.5.2 Factsheets and Advisories

- Records Management Factsheet 04 – Managing Emails and Other Modern Media – **www.port.ac.uk/departments/services/corporategovernance/recordsmanagement/factsheets/**
- Information Security Advisories – **http://ithelp.port.ac.uk/questions/422/Information+Security+Advisories**

1.5.3 Google policies

- Google Apps Acceptable Use Policy – **www.google.com/apps/intl/en/terms/use_policy.html**
- Google Privacy Policy – **www.google.co.uk/policies/privacy/**

1.5.4 Third party policies

- Safe Harbor Framework – **www.export.gov/safeharbor**
- JANET Acceptable Use Policy – **https://community.jisc.ac.uk/library/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 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, as Google Apps is web-based and can be accessed from any location with internet access. This is to ensure that the University has a record of all business correspondence and to enable the University to back up work-related emails for business continuity purposes. In addition, provision has been made for offline access to emails, when necessary.

Emails are subject to the same laws and policies that apply to other forms of communication, including the Data Protection Act 1998 and the Freedom of Information Act 2000, and must be composed using the same degree of care as would be used for a formal letter. Emails and instant messages (which are saved in Google Apps, if one or more of the people involved in the conversation have the history set to 'on the record') are potentially disclosable to external parties and statements must not be made that could expose the University to legal liability or damage its reputation.

All communication undertaken on behalf of the University is subject to the University's Anti-Bullying and Harassment Policy (available at **www.port.ac.uk/accesstoinformation/policies**), which espouses the principles of respect and dignity in all correspondence.

Staff should ensure that their electronic work diaries are held within Google Apps Calendar 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 Google Apps Acceptable Use Policy (available at **www.google.com/apps/intl/en/terms/use_policy.html**).

2.1 Security

Users are responsible for the security of their mailboxes.

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 software is installed and maintained on any computer used to gain access to the University's IT facilities. (Free antivirus software can be downloaded from **http://ithelp.port.ac.uk/**, search for Antivirus.)

Google Apps 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 at **http://ithelp.port.ac.uk/questions/422/Information+Security+Advisories**.

Users may not monitor, intercept or browse the messages of others, unless authorised to do so. The IS Service Desk should be informed immediately, if a suspected virus is received or a user becomes aware that someone has gained unauthorised access to his/her account.

Google Mail automatically helps identify spam and suspicious emails and will place these into your Spam folder (label). Staff can also teach Google Mail what is spam by highlighting emails in your inbox and clicking 'Report Spam' button. This will send the message to your Spam folder and remove it from your inbox, and Google Mail will continue to do the same if you receive future emails from that sender. If you make a mistake and don't want the message to be in Spam, click the 'Not Spam' button to move it back into your inbox.

Staff should lock their work stations (ctrl+alt+del on Windows) when away from their desk, even for short periods. Computers which cannot be locked must not be left unattended whilst logged-on.

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;
- 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;
- excessive or unreasonable personal use (see section 2.3 below).

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.

2.3 Personal use

Modern technology makes it easy to check personal email accounts on mobile devices, anywhere, anytime. Therefore staff are now encouraged to use personal email accounts for personal emails. Staff are permitted a reasonable level of personal use within their work email account, but it must not:

- be detrimental to the main purpose for which the facilities are provided;
- conflict with University objectives, values, or interests;
- conflict with the University's rules, regulations, policies and procedures;
- conflict with an employee's obligations to the University as their employer;
- involve personal financial gain or be of a commercial or profit-making nature (e.g. Avon campaigns, or advertising services that could take the individual away from their own work)*;
- involve significant use to pursue personal legal or domestic issues.

*However, appropriate use of email in conjunction with the Staff Noticeboard facility is permitted at **www.port.ac.uk/staffessentials/generalinformation/thenoticeboard/termsandconditions/**.

Staff should ensure that any messages addressed to or sent from their work email account for private purposes are clearly identified as personal and filed within a separate folder. Separating personal emails from work-related information will help delegated access users to avoid breaching the privacy of others when checking mail on behalf of absent members of staff.

2.4 Delegated access

Staff should give at least one colleague delegated access (formerly known as proxy access) to their account, so that business emails can continue to be answered in cases of unexpected or prolonged absence. Staff should be aware that when they allow a colleague delegated access within Google Mail, they are granting full read and write access to that person. However, any emails sent from an email address using delegated permissions will clearly identify the real author to the recipient.

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 and must not view data that is clearly of a personal nature. For further guidance, please see 'Guidelines for Dealing with Email and Post in Cases of Staff Absence', a set of guidelines which have been agreed with the Unions (available at **www.port.ac.uk/accesstoinformation/policies**).

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 so that staff do not become resistant to receiving information through its over-use.

Weekly all-staff emails are distributed on a Friday afternoon. Further details on the submission of appropriate content for the weekly bulletins are available at **www.port.ac.uk/staffessentials/generalinformation/staffcommunications/email/**.

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

- Members of the University Executive Board (UEB)
- Director of Information Services (or IS Service Desk)
- Internal Communications Manager
- 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 *ad hoc* 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 operation or suspension of IT systems
- Health and safety matters
- Access issues where buildings may be affected
- Strategic and operational information from UEB
- Governance matters
- Critical incidents

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

2.6 Monitoring

Account activities (e.g. storage usage, number of log-ins) are monitored by Google and all messages are routinely scanned (for viruses, spam and other security threats) to assist with the effective operation of the email system. This process is completely automated and no human intervention is involved. The use of all personal information by Google is governed by its Privacy Policy (**www.google.co.uk/policies/privacy/**).

The University, as the domain administrator for Google's facilities, may have access to information held in an email 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 and evidenced 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.

This list is not exhaustive. Any University monitoring that takes place will be conducted by IS staff, authorised by the Director of Information Services, and will be in line with the requirements of the Information Commissioner's Office – Employment Practices Code. Where there is evidence of an offence, it will be investigated in accordance with the University's disciplinary procedures. The University reserves the right to demand that encryption keys, where used, are made available, so that it can gain access to relevant emails as part of an investigation.

2.7 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 it via email. If any documents containing sensitive information need to be sent from the University's network to external addresses, staff are advised to encrypt them. (For guidance on how to encrypt documents please contact the IS Service Desk on extension 7777 or **servicedesk@port.ac.uk**. Annex A of the Data Protection Policy, available at **www.port.ac.uk/accesstoinformation/policies**, 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

Work-related emails are records of the University's actions and decisions, and must be managed as efficiently 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 Labels, Stars and importance tags to aid the management of current mail and retrieval of archived mail.

3.1 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: **https://storage.googleapis.com/edm-email-content/EmailSignatureInstructions.pdf**.

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.

3.2 Retention

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.

The risk implications of deleting messages must be considered, as well as the obligation to comply with the Fifth Data Protection Principle ('personal data processed for any purpose or purposes shall not be kept for longer than is necessary'). All emails that are retained will be subject to Data Protection and Freedom of Information legislation, and may be legally admissible.

3.3 Deletion

Google offers unlimited email storage, but this must **not** be abused. Users are still 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 30 days and cannot be recovered. For further guidance on managing emails, please see the Help pages at **http://mail.google.com/support/?hl=en**. Whilst information is held in the Bin, it will be considered still accessible and may therefore have to be released (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 email account (formerly known as generic accounts). 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.

3.5 Instant messages

Instant messaging is provided by Google Apps Hangouts. Instant messages are saved in Google Apps, if one or more of the people involved in the conversation have the history set to 'on the record'. This means that instant messages are potentially disclosable to external parties in response to requests made under the Freedom of Information or Data Protection legislation.

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. For further guidance, please see the 'Guidelines for Dealing with Email and Post in Cases of Staff Absence', as agreed with the Unions (available in the Document Warehouse at **www.port.ac.uk/accesstoinformation/policies**).

3.6.2 Illness

In cases of illness, where it is not possible to make any preparations for being away from the office, staff should 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 (who, in the case of academic staff, must be the Head of Department) 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, he/she should follow the procedures specified by the Information Security Advisory on third party access to email (available at http://ithelp.port.ac.uk/questions/422/Information+Security+Advisories)

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 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; it is therefore important that they remove all their personal emails – any items of a personal nature that they wish to retain should be forwarded to a private email address in advance of their departure.

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 at **www.port.ac.uk/accesstoinformation/policies**).

3.8 Further information

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

- Email: **servicedesk@port.ac.uk**
- Telephone: 023 9284 7777
- Website: **http://ithelp.port.ac.uk/**

For guidance on using Google Mail, please visit the help pages at:

- **http://mail.google.com/support/?hl=en**

Appendix

Legislation

1. Copyright

Email messages and attachments are subject to the laws regarding copyright, including the Copyright, Designs and Patents Act 1988. Users must ensure that they do not circulate or store material that infringes the intellectual property rights of a third party. For further guidance, please consult the University's Copyright Code (**www.port.ac.uk/accesstoinformation/policies**).

2. Data protection

The Data Protection Act 1998 covers personal data that can identify a living individual and relates to not only facts but also opinions. Under this legislation, individuals have the right to ask to see the personal data held about them. Care should therefore be taken in writing emails that may contain personal data as the emails, whether held in an individual's email account or on the University server, will have to be released if requested. More details about data protection can found at **www.port.ac.uk/dpa**, including a copy of the University's Data Protection Policy (**www.port.ac.uk/accesstoinformation/policies**).

3. Defamation

Email is a form of publication and therefore the laws of defamation and libel apply. Material to be transmitted via the email system must be free from such statements: it should not contain anything that could be seen as insulting or damaging to the personal or professional reputation to an individual or a group of people.

4. Discrimination

Users must ensure that they do not include comments that could be considered discriminatory under the terms of the Equality Act 2010.

5. Freedom of information

The Freedom of Information Act 2000 allows anyone access, on request, to a great deal of information held by public authorities. The University is defined as a public authority and therefore must respond to any requests for information (unless an exemption applies which prevents disclosure) within 20 working days of receipt of the request. Information 'held' by the University includes all emails, sent from or to a University address. Also includes work-related emails sent from or to a staff member's private email address.

It is also important that if a member of staff is away from the University for more than two days, they should use an out-of-office message telling the sender to whom they can forward their email if they want a reply before the member of staff returns to the University. Failure to use an out-of-office message means that the email is received by the University the moment it enters the University system and the 20 working days start from that time, even when the email may not be opened for some time after that. For more information on this aspect of the legislation please see the 'Guidelines for Dealing with Email and Post in Cases of Staff Absence' (**www.port.ac.uk/accesstoinformation/policies**).

The University has more information on the Freedom of Information legislation at **www.port.ac.uk/accesstoinformation/freedomofinformation**.

6. Hacking

Hacking activities are offences under the Computer Misuse Act 1998, as amended by the Police and Justice Act 2006. Under the terms of this legislation, it is an offence to gain unauthorised access to any program or data held in a computer, and to impair the operation of programs or the reliability of data.

7. Harassment

Messages must be free from any content that could be considered harassing, threatening, abusive or insulting. Content of this type is an offence under the Criminal Justice and Public Order Act 1994 and the Protection from Harassment Act 1997, as well as the Malicious Communications Act 1998. For further details about harassment, please see the University's Anti-Bullying and Harassment Policy (available in the Document Warehouse at **www.port.ac.uk/accesstoinformation/policies**).

8. Obscenity

It is a criminal offence to publish any material that is pornographic, excessively violent or that comes under the provisions of the Obscene Publications Act 1959. Similarly, the Protection of Children Act 1978 makes it an offence to publish or distribute obscene material of a child.

University of Portsmouth
Directorate
University House
Winston Churchill Avenue
Portsmouth PO1 2UP
United Kingdom

T: +44 (0)23 9284 3195
F: +44 (0)23 9284 3319
E: corporate-governance@port.ac.uk
W: www.port.ac.uk

MD10648 0915