

STUDENT EMAIL POLICY

August 2025

Contents

Summary.....	4
What is this document about?	4
Who is this for?.....	4
How does the University check this is followed?	4
Who can you contact if you have any queries about this document?.....	4
Policy	5
1. Introduction.....	5
2. Acceptable use	6
3. Managing email accounts.....	8

Document title		
Student Email Policy		
Document author and department		
Sarah Arnold, University Records Manager, Corporate Governance		
Approving body		
Paul Mould, Executive Director of Corporate Governance		
Date of approval		
13/08/2025		
Review date		
August 2028		
Edition no.		
7		
ID Code		
146		
Date of effect		
18/08/2025		
EITHER For public access online (internet)? <i>Tick as appropriate</i>		YES
For public access on request copy to be mailed <i>Tick as appropriate</i>		YES
OR For staff access only (intranet)? <i>Tick as appropriate</i>		
Password protected <i>Tick as appropriate</i>	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-146.pdf>

Summary

What is this document about?

The purpose of this Policy is to set out the conditions under which the University's email system may be used. From September 2025 Students will be using Microsoft 365, but some older alumni may still be using Google Workspace for Education. For the avoidance of doubt, where this policy references Google or Microsoft, students 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 students who use a University email account (@myport.ac.uk email addresses), as well as former students (alumni) who continue to use their accounts.

The use of staff accounts (@port.ac.uk email addresses) by staff and other authorised account holders, including PhD students, is covered by the Staff Email Policy which can be found in the [policy section](#) of the University website.

How does the University check this is followed?

Regular internal audits are planned and carried out to check compliance with existing policies.

In addition, Library and Information Services (LIS) monitor emails, both incoming and outgoing, to protect sensitive data and improve operational efficiency.

Students will be reminded of the need to manage their emails effectively via an annual All Students email.

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](#).

Policy

1. Introduction

The University provides all students with an email account in order to have one dedicated channel of communication with them. The purpose of this Policy is to set out the conditions under which the University's email system may be used. It applies to all students who use a University account, as well as alumni who may continue to use their accounts for up to 2 years from the completion of (or withdrawal from) their studies.

1.1. Responsibilities

All users of the University's email system are responsible for the security of their mailboxes and must not disclose their passwords to others. They are also responsible for all activities that occur within their accounts. If a user becomes aware that any unauthorised access has taken place, they should notify the Library & Information Services (LIS) [Service Desk](#) immediately.

Any emails sent by the University to students will be delivered to their UoP addresses and students must ensure that they check their accounts regularly. Any member of staff, who is enrolled as a student, must not use their student email account to conduct University business. Their staff email account should be used for this purpose, as required by the Staff Email Policy.

Responsibility for reviewing and updating this Policy lies with the University Records Manager, authorised by the Executive Director of Corporate Governance. All account holders are expected to comply with the Policy, and staff with responsibilities for students should be aware of its requirements.

1.2. Ownership

The University provides all students with Microsoft 365 accounts for the duration of their studies. Access to OneDrive and Teams will be removed at the point the student leaves, to enable their licence to be reused for future students. Alumni will be moved to an A1 licence which will permit them to continue to use their **email only** for up to 2 years from the completion of (or withdrawal from) their studies. After this time their email address will also be retired from use.

Students should be aware that every email address and associated account – whether used by a current or former student – is the property of the University and is provided solely for the purpose of assisting with studies.

From September 2024, students must not use their email address and associated account for non-University business. All existing personal emails and any items of a personal nature that they wish to retain from their account must have been removed by the end of 2024 or before the closure of their account, whichever was the sooner. It is highly inadvisable for students to link any personal devices or personal logins to their @myport.ac.uk account in a way which would prohibit their use of that personal device or login when their account is closed. It is also highly inadvisable for students to purchase media items (such as music or movies) using their @myport.ac.uk account, as this data may not be transferable to another account for copyright reasons, so would be lost when their account is closed.

1.3. Data Protection

The University acts as the domain administrator for both 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 defamation, harassment, copyright and data protection.

1.5. Related policies

This Policy should be read in conjunction with the following policies and guidance available in the [policy section](#) of the University website:

- Code of Student Behaviour
- Dignity and Respect Policy
- Data Protection Policy
- ICT Acceptable Use Policy
- Information Security Policy

As well as the following Google policies:

- [Google Workspace for Education Acceptable Use Policy](#)
- [Google Privacy Policy](#)

And the [Microsoft Product Terms](#), covering:

- Microsoft Acceptable Use Policy
- Microsoft Privacy Policy

2. Acceptable use

Authorised users of the University's email system must use its facilities responsibly, complying with all relevant policies and laws.

2.1. Acceptable Use Policies

The University has an ICT Acceptable Use policy available in the [policy section](#) of the University website. In addition, students are also expected to comply with the acceptable use policies of both Google and Microsoft. These policies are linked from section 1.5 above.

2.2. Prohibited use

The University's email system must not be used for:

- the creation, transmission or storage of text, images and other material that is offensive, obscene, indecent, discriminatory, harassing or libellous;
- 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 incitement of violence;
- 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;
- unauthorised personal financial gain or a commercial or profit-making nature, e.g. trading on eBay.

This list is not exhaustive. Contravention of any of the above terms (listed in sections 2.1 to 2.2) may result in the suspension or termination of a user's access to facilities. The instigation of formal action under the University's disciplinary procedures may follow and, in certain circumstances, legal action may be taken.

2.3. Security

Students are responsible for the security of their mailboxes and must not disclose their passwords to others. In addition to a strong password, the University requires the use of multifactor authentication ([two-step verification](#)) for Google and Microsoft accounts.

Although emails are routinely scanned for virus content and spam, students 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 clicking on any links from unsolicited or untrusted sources
- Not transmitting attachments known to be infected with a virus;
- Not forwarding any suspicious emails regardless if they contain attachments or not
- Ensuring that antivirus/anti-spyware software is installed and maintained on any computer used to gain access to the University's IT facilities.
- Ensuring proper disposal of printed emails, especially those marked "for your eyes only", "confidential" or "sensitive"
- Avoid sending sensitive information via email unless encrypted and indicated that the email is of a sensitive / confidential nature in a subject of the email.

The unauthorised interception of, or access to, the messages of others is illegal.

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 their account.

2.4. Monitoring

The University will carry out monitoring to guard against cyber-attacks. This routine 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:

- to investigate a complaint, where relevant;
- to investigate a reasonable suspicion of abuse of computer facilities;
- to cooperate in the investigation of a crime;
- to comply with legal responsibilities;
- in an emergency situation, including as a response to a potential cyber incident.

Otherwise, the University will respect the privacy of all account holders.

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.

2.5. Authorised Research

Research is part of the core business of the University. From time to time students 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.

3. Managing email accounts

3.1. Email addresses

Each student will be provided with an email account at the time of enrolment. The address for the account will be based on the individual's student number (e.g. UP123456@myport.ac.uk).

3.2. Managing accounts

Messages that users still require, but wish to remove from their inbox, can be archived, while messages that are no longer needed should be deleted. Users should be aware that deleted items will be automatically emptied after thirty days and cannot be recovered.

All emails sent by the University to students will be delivered to their MyPort email addresses, and it is important that the accounts are checked regularly. Students may choose to forward Moodle email to their MyPort email address.

Although Microsoft 365 may be used by students for collaborative purposes, any group project work that needs to be assessed and marked must be transferred to Moodle so that it will be accessible to tutors.

3.3. Further information

For further information about email accounts, please contact the Service Desk:

- [Service Desk](#) Web Form
- Telephone: 023 9284 7777

- For guidance on using Microsoft, please visit the Microsoft [support site](#).
- For guidance on using Google Mail, please visit the Google [help pages](#).

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

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