

# IT04 - Email and Instant Messaging Usage Policy

## Introduction

- 1 This policy sets out the general rules for the use of Solent University's email and Instant Messaging (IM) systems. The University's email and IM systems are coordinated and managed by Information and Communications Technology (ICT). No other email or IM system (server or client) is recognised by or supported within the University.
- 2 It is the responsibility of each individual user to ensure that they use University IT services in an acceptable manner in accordance with all University policies and current legislation.

## Executive Summary

- 3 The key elements of the Email and Instant Messaging Usage Policy are:
  - i All University email addresses and associated accounts are the property of the University.
  - ii Unless special measures are undertaken, all emails sent to external recipients should be regarded as having the same security status as a postcard.
  - iii All University-related email and IM chat correspondence must be conducted using the University's email and IM systems - Microsoft 365 email/calendar system and Microsoft Teams.
  - iv All University emails and logged IM chat messages are subject to the General Data Protection Regulation, the Data Protection Act 2018, and the Freedom of Information Act and may be legally disclosable.
  - v All users working in a staff-capacity (hereafter referred to as staff) are responsible for ensuring that any work-related emails are kept according to the University's Records Management and General Data Protection Regulation policies.
  - vi Users are permitted to use the University's email and IM systems for occasional personal use.
  - vii When staff leave the University, it is their responsibility to transfer to appropriate colleagues or their line manager any emails that need to be retained.
  - viii Staff should ensure that their calendar in the University's email system is kept up-to-date so that colleagues can easily confirm their availability when booking appointments and arranging meetings.

## Ownership

- 4 The associated accounts and their stored data within the University's Email and IM systems are the property of the University which allows the University the right, where necessary, to monitor/access emails and IMs.

## Email Address Format

- 5 Staff and affiliate user email addresses are automatically allocated to users using the format `knownas.lastname@solent.ac.uk` where `knownas` is the user's preferred forename and `lastname` is the user's surname as stored in the People and Development/Payroll system or Affiliate Management System. If this would cause a match to an existing email address then the user's middle initial is checked to see if this would allow the creation of a unique email address. If no middle initial is available or it would match an existing email address then the format `knownas.lastnameN@solent.ac.uk` is used where `N` represents a number from 2 upwards which will allow the creation of a unique email address.
- 6 Student user email addresses are automatically allocated to users using the format `username@solent.ac.uk` where `username` is a unique identifier created using the user's information from the Student Records System.
- 7 Postgraduate research students are automatically allocated an email address using the student email address format. However they can request, via the Postgraduate Research Support Officer, to have their allocated email address changed to the staff/affiliate email address format. The Postgraduate Research Support Officer will verify the request and pass it on to the ICT Service Desk. The original requester will be allocated the first available staff/affiliate format email address using their details and their student format email address will be retained as an alias such that emails sent to their student format email address can still be delivered to them.

## Shared Mailboxes




- 8 Where several users are responsible for the same area of work and require access to the same emails then a member of the management team within the relevant Faculty/School/Service may request to the ICT Service Desk for the creation of a shared mailbox with an associated, generic, email address that represents the shared area of work. The request must include the name of the person who will be in overall management of the shared mailbox and the names of the other users who require access.
- 9 An email address allocated to a shared mailbox must be generic enough so that it encompasses the area of work shared by the users accessing that mailbox but it must not be so generic that there would be an overlap with users performing a similar role in another part of the University who would not have access to that shared mailbox.
- 10 A shared mailbox does not have an associated username and password as users must log on with their personally-allocated username and password. This will give them access to their own mailbox and to the shared mailbox.

## Security

- 11 Disk/storage encryption must be enabled on any device running an email/calendar app that creates local storage of university email/calendar data.
- 12 All access to the University's Microsoft 365 email/calendar system must be via a university permitted email/calendar app running on a permitted device, with

access to that device protected using a password/PIN (or similar) that is not shared with anyone else.

- 13 For compliance with cyber security standards/certifications (such as Cyber Essentials), mandatory security measures may be enforced via the University’s Mobile Application Management service.
- 14 A summary of permitted email/calendar apps for accessing the University’s Microsoft 365 email/calendar system, what devices they can be used on, and where disk/storage encryption must be enabled is shown in the following table:

		Microsoft 365 - Permitted Email/Calendar Apps			
		Web browser access  ( <a href="#">Outlook Web Access</a> and <a href="#">MySolent</a> )	Outlook desktop app* 	Outlook for <a href="#">Android/iOS</a>  or MySolent for <a href="#">Android/iOS</a> 	Any other email or calendar app
<b>Device</b>	ICT-managed staff build laptop/desktop (Windows 10 and macOS)	Yes	Yes*	Not applicable	No
	ICT-managed student/shared build laptop/desktop (Windows 10 and macOS)	Yes	No	Not applicable	No
	Mobile device (Android or iOS only)	Yes**	Not applicable	Yes**	No
	Any other device	Yes**	No	Not applicable	No

\*The Outlook desktop app is only permitted to be used on ICT-managed staff build devices due to the security controls needed to protect locally cached university data.

\*\*Provided storage encryption is enabled and access to the device is protected using a PIN (or similar) to prevent unauthorised access.

- 15 All emails arriving at the University are scanned for computer virus and spam (unsolicited bulk email) content before delivery and any matching emails are rejected. However, email scanning can never be 100% accurate. Additionally, attachments sent via IM are not virus scanned during transfer so users are expected to take suitable measures to ensure that they prevent the introduction and transmission of computer viruses. Some guidelines are listed below but please contact the ICT Service Desk if you require advice:

- i Do not open attachments received from unsolicited or untrusted sources.
- ii Be wary of unsolicited attachments. If in doubt, contact the sender to check before opening the attachment.
- iii Do not email/IM attachments known to be infected with a virus.
- iv Check that suitable anti-virus software is installed on the computer you’re using and that it’s up-to-date.

- 16 If you believe that you have received a phishing email/message in Microsoft Outlook/Teams then please report it as 'Phishing' using the built-in "Report as" functionality within Microsoft Outlook/Teams. If you have engaged with a phishing email/message - replied to it, forwarded it, clicked on any links in it, or opened any attachments - then you must report it as a suspected information security incident.
- 17 Suspected or actual information security incidents must be reported as soon as possible, by completing the [Information Security Incident Notification form](#) and emailing it to [InfoSec@solent.ac.uk](mailto:InfoSec@solent.ac.uk). More guidance can be found in the [Information Security Incident Management Policy](#).
- 18 Although the University uses (where available) secure methods for email transmission and user access, email confidentiality cannot be guaranteed. Unless special measures are undertaken by the user, all emails sent to external recipients should be regarded as having the same security status as a postcard and personal, confidential or sensitive information should not be sent in the body of an email or in its Subject. Where there is a business need to send personal, confidential or sensitive information via email then the information must be encrypted before it is attached to the email. For guidance on how to encrypt documents please contact the ICT Service Desk.
- 19 Credit card information must never be sent via email/IM or asked to be sent via email/IM. Any credit card information received via email/IM must be immediately deleted by the recipient and must not be printed, copied, replied to, forwarded on or processed for payment. The sender must be informed that no payment was taken, their credit card details were deleted and that they must use an approved method of payment. The incident must also be reported to the ICT Service Desk as there are further processes needed to remove the data from our systems.

## Email and IM Account Usage

- 20 In relation to email and IM, the following uses are specifically excluded:
  - i The sending of bulk email/IM, including excessive use of mailing lists, which is unrelated to the legitimate academic or administrative activities of the University and is likely to cause offence or inconvenience to those receiving it.
  - ii The sending of sensitive messages using email/IM, for example employment decisions. If in doubt, alternative methods of communication should be employed, or advice sought.
  - iii Subscribing to external web sites and mailing lists using your University email address for personal use not related to your University work/study. For example: Amazon, Ebay, Facebook etc.
- 21 Staff must always use their University email and IM account to conduct University business. The University's email and IM systems can be securely accessed from any location with Internet access and offline email usage is also possible. Staff are not permitted to auto-forward emails from their account to other email systems.
- 22 Students must use their University email and IM account to conduct University-related correspondence. The University's email and IM systems can be securely accessed from any location with Internet access and offline email usage is also

possible. Students are not permitted to auto-forward emails from their account (even to other Solent University email addresses).

- 23 All emails sent from the University to students must always be sent to the student's University email address. Staff receiving non-University emails purporting to have been sent by a student should treat such emails with caution and always reply to the student's University email address.
- 24 Staff who are also enrolled as a student must ensure that they use their staff account to conduct University business. Similarly, any emails sent in their capacity as a student must be sent from their student account.
- 25 Before leaving the University, users should unsubscribe from any email lists they have subscribed to and delete any personal emails in their account. If there are any work-related emails that need to be transferred to another user then the built-in delegation features should be used so that these emails can be transferred from one account to another. On their last working day Staff should enable Microsoft Outlook's "Automatic Replies" feature with no end date specified and a message stating that they have left the University and who the sender should contact instead.
- 26 Following the departure of a member of staff from the University, their email account will be closed for access by them and deleted after a period of 56 days. University management may request access to be given to the closed mailbox by another member of staff for this duration.

## **General Data Protection Regulation, Data Protection Act and Freedom of Information Act**

- 27 As well as the guidelines outlined in the ICT Security Policy and the Data Protection Policy, the following guidelines are specific to email and logged IM chats:
  - i Under the General Data Protection Regulation and the Data Protection Act 2018, all email transmissions and logged IM chats which contain personal data may be disclosed in response to a request for disclosure, brought forward (through normal procedure), via the University's Data Protection Officer.
  - ii 'Personal data' can include a sender's opinion of another person.
  - iii The University's internal and external use of email systems, for bona fide purposes connecting with its operations, is registered with the Data Protection Registrar.
  - iv The University's correspondent with the Information Commissioner concerning the use of email, shall be the Data Protection Officer.
  - v On a day-to-day basis, the Data Protection Officer shall devolve responsibility for Data Protection matters concerning email.
  - vi The use of email, as a means of internal as well as external communication, falls within the provisions of the General Data Protection Regulation and the Data Protection Act 2018.

vii Under the terms of the General Data Protection Regulation and the Data Protection Act 2018, email users who have access to email addresses have a responsibility not to disclose email addresses or email distribution lists to an unauthorised third party without permission of the owner of the email address.

28 Emails and logged IM chats are also potentially subject to disclosure under the Freedom of Information Act.

29 Instant messaging should only be used for informal communications with colleagues - any discussions pertinent to the University's business should be conducted via email so that a formal record exists.

## Retention

30 All users working in a staff-capacity are responsible for ensuring that any work-related emails are kept according to the University's Records Management Policy and General Data Protection Regulation (GDPR) Policy.

## Email Distribution Lists and Mass Emails

31 Email distribution (group) lists provided by the University must only be used for matters of University business. To send to such a distribution list the sender must be either an administrator/moderator of the distribution list, a member of the distribution list or, for course lists, a member of staff involved with that course. Any multiple use of email distribution lists provided should be avoided unless absolutely necessary.

32 Prior permission from the Vice Chancellor's Office is required to send a message to all staff or to all students.

33 A valid 'Reply-To' address must be used on any mass email with additional contact details given in the body of the email.

34 Do not put the name of the distribution list or a large list of names in the 'To' or 'Cc' fields but use the 'Bcc' field instead. This ensures the list of recipients will not be displayed when the email is sent out and prevents recipients from accidentally sending their reply to the whole list.

35 The 'Subject' line must be clear and concise. An email to all staff must include the prefix 'All Staff: ' and an email to all students must include the prefix 'All Students: '.

36 The body of the email should be as brief as possible and clear and unambiguous.

37 Do not send mass emails with attachments but try to contain the information within the body of the email or, as a last resort, in a web link. Where a web link is used then it must also provide information as to how the linked content can be accessed manually without clicking on the link. This is to help the recipient distinguish the email from a malicious 'phishing' email.

38 The Faculty/School/Service email distribution lists ('GRP\_' prefix) are maintained by ICT and are automatically populated using information from the People and Development or Affiliate User Systems. These email distribution lists are not manually alterable.

- 39 The course email distribution lists ('Course\_') are prefix maintained by ICT and are automatically populated using information from the Student Records System. These email distribution lists are not manually alterable.
- 40 The general email distribution lists ('LIST' prefix) are provided for Faculty, School, or Service use and are maintained by the relevant Faculty/School/Service. A member of the management team within the relevant Faculty/School/Service may request to the ICT Service Desk for the creation of an email distribution list. The request must include the name(s) of the person(s) who will be in overall management of the email distribution list. Please note that such lists should not contain external (non-University) email addresses unless the title of the list makes it very clear to a sender using the list that it contains external recipients.

## Code of Practice

- 41 All users should adhere to the following guidelines for appropriate use:
- i Check your email regularly - once a day is an absolute minimum. For staff users, depending on the nature of the post, email may need checking on a more regular basis. Students must recognise that certain communications may be time critical. "I didn't check my email", and errors in forwarding, user unknown or other error messages are not acceptable excuses for missing official University communications sent by email.
  - ii Do not expect a recipient to be constantly checking their email/IM or be available to respond immediately. If you require an immediate response then email/IM is not the correct method of communication and you should use a phone call instead, ideally to a relevant role-based telephone number provided for such purposes e.g. the ICT Service Desk on 023 8201 2345.
  - iii If you use the 'Urgent' feature in email then it lets the recipient know that you consider the matter to be urgent. However, the recipient has their own workload to manage and, as such, the email may not be deemed urgent by them.
  - iv The use of 'Delivery Receipt' or 'Read Receipt' on an email can be deemed to imply a lack of trust in the recipient and so should not be used unless absolutely necessary. It should be noted that a 'Delivery Receipt' or 'Read Receipt' response is not guaranteed and may be blocked by the recipient's email system or the recipient's email client.
  - v Be polite. Messages sent by email/IM can often seem abrupt, even when this is not the intention. Use professional courtesy and discretion. The use of all upper-case text in either the subject or the body of an email/IM should also be avoided as this is deemed to be the equivalent of shouting.
  - vi Before you send an email/IM, read it through to make sure it really does say what you want it to say.
  - vii Do not say anything in an email/IM that you would not be prepared to say to someone face to face.
  - viii Do not reply "With History" if it is not necessary especially if it incorporates a large attachment.

- ix Use 'reply all' and distribution lists with caution in order to keep the number of messages to a minimum and reduce the risk of sending messages to the wrong people.
  - x Messages should usually be addressed to those from whom an action or response is expected, with 'Cc' or 'Bcc' used for other recipients for whom the message is for information only. However, when you are sending an email to a large number of recipients or where the recipients must not know who else the email has been sent to (e.g. for personal data protection reasons) then 'Bcc' must be used.
  - xi Respect peoples' privacy and consider this aspect before forwarding messages.
  - xii Delete unwanted or unnecessary email. It is the user's responsibility to manage their email folders and keep within the set quota limits.
  - xiii Do not try to carry out confidential or sensitive tasks or express controversial views via email/IM.
  - xiv Enter a meaningful title in the 'Subject' field at the top of an email to help the reader anticipate the content correctly. Try to keep to one subject per message to help avoiding unnecessary confusion.
  - xv Don't use all or part of someone else's message without acknowledgement.
  - xvi Don't edit someone else's message without making it clear what the changes are that you have made. Don't distribute other people's messages without permission.
  - xvii Avoid subscribing to unnecessary mailing lists. Unsubscribe from mailing lists when they are no longer required.
  - xviii Do not forward email/IM "chain letters". These are emails/IMs which either ask you to forward them on to all your friends (or to everyone you know) or which state that something bad will happen if you do not forward them. Emails/IMs of this type, which are warning about something (e.g. computer viruses), are almost certainly hoaxes. If you are unsure about any email/IM that you've received then:
    - a Students can contact IT Support staff or the ICT Service Desk for information and help.
    - b Staff can contact the ICT Service Desk for information and help.
- 36 Staff are required to use the approved University email signature for all email communications. In order to do this, guidance can be found on the staff Portal at:

<https://staff.solent.ac.uk/our-organisation/solent-brand>

The email signature will be based on two formats:

- a HTML (Primary) - this is the main format and will use low resolution images as well as provide links to social channels.



- b Text (Secondary) - this is the secondary format and should only be used when HTML formats are not supported.

No other information should be added to email signatures. Any variation of this email signature needs written confirmation from the External Relations service.

- 37 Staff users should ensure that their calendar in the University's email system is kept up-to-date so that colleagues can easily confirm their availability when booking appointments and arranging meetings.

## **Out-of-Office Message**

- 38 Staff users must set an Out-of-Office message when they are away stating an alternative email contact for work-related matters.

## **Other Sources of Information**

- 39 Other University IT policies:

- i IT01 - IT Acceptable Use Policy.
- ii IT02 - IT Security Policy.
- iii IT03 - Internet Usage Policy.
- iv IT05 - Telephone and Mobile Phone Usage Policy.
- v IT06 - IT Hardware and Software Policy.
- vi IT07 - Disposal of IT Equipment and Media Policy.
- vii IT08 - Application Systems Policy.
- viii IT09 - Identity Management Policy.
- ix Information Security Incident Management Policy.

<https://students.solent.ac.uk/documents?document-type=strategy-policies-procedures-and-guidelines>

<https://staff.solent.ac.uk/documents?document-type=strategy-policies-procedures-and-guidelines&department-owner=information-and-communications-technology>

- 40 Other University policies, including but not limited to, the following:

- i General Data Protection Regulation (GDPR) Policy.
- ii Freedom of Information Policy.
- iii Records Management Policy.

<https://students.solent.ac.uk/documents?document-type=strategy-policies-procedures-and-guidelines>

<https://staff.solent.ac.uk/documents?document-type=strategy-policies-procedures-and-guidelines>

Solent University's Internet connections are governed by Jisc's network and technology policies: <https://community.jisc.ac.uk/library/janet-policies>

Author(s):	Keith Baker, ICT Security and Standards Manager
Approved by:	Gareth Roberts, Director of Digital Transformation
Date of approval:	29 April 2024
Version:	6.0
Next review date:	September 2025