

GISP6. Use of email

Date:	5 October 2017
Version:	2.0
Authors:	Raymond Scott
Quality Assurance:	Information Strategy and Services Committee (ISSC)

Version control

Revision	Date	Revision Description
1.0	8/11/12	Approved by ISSC
1.1	5/10/17	Reviewed and updated
2.0	20/10/17	Approved by ISSC

Policy

Security Control	University Email service for secure email correspondence.
Objective	To provide a secure and confidential email service for both staff and students.
Policy	<p>6.1. The University will provide a secure email service for all members of the University.</p> <p>6.2. An individual's email will be secure against unauthorised access by other individuals via the use of individual usernames and passwords (see GISP4 and GISP5).</p> <p>6.3. Anti-virus mechanisms will be implemented on the University's email gateways to help prevent virus infected email attachments reaching a user's inbox (see also GISP10, 'Protection against malicious software').</p> <p>6.4. Anti-spam mechanisms will be implemented on the University's email gateways to aid in reducing the volume of unsolicited email reaching a user's inbox.</p> <p>6.5. The University reserves the right to access an individual's University email account in the course of investigating a breach of University regulations, where illegal activity is suspected, or in the case of unexpected absence by staff, to ensure University business is not delayed or hindered (see Conditions of Computer Use).</p> <p>6.6. If confidential data is being transmitted via email, senders should ensure that this is sent in an encrypted format, or as a password protected attachment with the password conveyed to the recipient by means other than email (e.g. by telephone) and that appropriate measures have been taken to ensure authenticity and confidentiality, that it is correctly addressed and that the recipients are authorised to receive it.</p> <p>6.7. Acceptable use of the University email services as defined in the Conditions of Computer Use.</p>
Responsibility	<ul style="list-style-type: none"> ITCS is responsible for providing a secure email service for staff and students. Individuals using provided email services must comply with the Conditions of Computer Use.

	<ul style="list-style-type: none"> • Individuals using provided email services should ensure that all emails are addressed correctly.
Incident Management	Any breaches of email security should be immediately reported to the IT Service Desk.
Implementation	<ul style="list-style-type: none"> • All users should follow the guidance on email best practice available from the web page https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/it-regulations-and-policies/user-guidelines/email-guidelines • Emails sent to parties outside the University should include the standard disclaimer notice https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/it-regulations-and-policies/user-guidelines/email-disclaimer-notice • Where appropriate, a confidentiality notice should be added to emails https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/it-regulations-and-policies/user-guidelines/email-confidentiality-notice