USE OF EMAIL CODE OF PRACTICE

1. INTRODUCTION

1.1. This Code of Practice should be read in conjunction with the University's Acceptable Use Policy.

1.2. The purpose of this Code of Practice is to outline the University's expectations of the use of its e-communication systems including Microsoft 356 email and its instant messaging elements such as Teams or Yammer.

1.3. The University has an obligation to comply with relevant legal and statutory requirements with regards to how the University uses and governs its e-communication systems and how it protects the data and information processed within and between those systems. The applicable laws include but are not limited to:

- Data Protection Legislation (DPA2018, UK GDPR, Privacy and Electronic Communications Regulations 2003 including Data Subject Access Requests)
- Freedom of Information Act 2000
- Copyright, Designs and Patents Act 1988
- The Copyright and Rights in Performances (Quotation and Parody) Regulations 2014
- Computer Misuse Act 1990
- Counter-Terrorism and Security Act 2015
- Prevent Duty Guidance: for Higher Education Institutions in England and Wales
- Public Interest Disclosure Act 1998
- Defamation Act 1996
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000)
- Other related legislation that may influence this Code of Practice

2. SCOPE

2.1 This Code of Practice applies to all users of a Keele IT account and applies to all staff, students, contractors, third party agents and visitors who access and use Keele e-communication systems.

2.2 It applies to the access and use of the University's e-communication systems, including Microsoft 365 email and its instant messaging elements such as Teams or Yammer. It applies to any University-supplied or personal device (PC, Apple, Linux, Mobile Phone) from which University systems are accessed whether on or off campus.

3. EXPECTATIONS OF USE

3.1 All use of the University's e-communication systems must be in line with the Acceptable Use Policy.

3.2 Staff should use Keele IT accounts to conduct Keele University business and should not use any other third-party IT accounts to conduct Keele University business.

3.3 For all staff automatic forwarding or redirection of email to external mail domains is not allowed. Automatic forwarding or redirection of email internally within the Keele.ac.uk mail domain is possible and it is the individual's responsibility to set forwarding up and make sure the forwarding address is correct.

3.4 For all students automatic forwarding or redirection of email to other mail domains is possible. All responsibility for email forwarded off the campus network remains with the individual. It is the individual's responsibility to set forwarding up and make sure the forwarding address is correct and the email service being used is reputable and reliable. Users must exercise caution when automatically forwarding any email to an outside network and question the need to even do so.

3.5 IT e-communications can be records of the University's actions and decisions and must be managed efficiently and securely in accordance with the Data Classification and Handling Policy. It is the responsibility of all staff to consider which e-communication channel is the most appropriate to use when sending / sharing data and to ensure that messages that constitute a record of business data are retained in an appropriate storage location in accordance with the University's Records Retention Schedule;

3.6 Your email account should not be used as a filing system, Microsoft365 allows users to save email messages and instant messages directly to Onedrive and Team folders.

3.7 Upon graduation, students IT accounts will be deleted after 365 days, any data required should be transferred prior to leaving. It is therefore important that students and alumni remove all their personal emails and any items of a personal nature that they wish to retain from their email account in advance of it being closed.

3.8 The University will maintain and include a standard disclaimer message in all University-generated emails which is updated by from time to time.

3.9 The University may at times monitor its e-communications systems and network. Please refer to the University's Acceptable Use Policy and Monitoring and Interception Policy for more detailed information on monitoring.

3.10 Failure to read an official email does not exempt a staff member or student from their responsibility to comply with the message.

3.11 Any emails sent by the University to students will be delivered to their O365 email address(es) 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.

3.12 Upon leaving the University, staff members IT e-communication accounts will be deleted after 30 days. Any data held in a personal area which may be needed by the University must be transferred to an appropriate shared space prior to departure. It is the staff member's responsibility to ensure that their mailbox is cleared out through deleting unwanted emails, making emails that have university business relevancy available to an appropriate work colleague and ensuring any email containing their own personal information are removed/deleted.

3.13 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 via emailed content in line with the requirements of the IT Acceptable Use Policy. These include:

- Users being wary of opening attachments from unsolicited or untrusted sources and checking links by hovering over the text.
- Not transmitting attachments known or suspected to be infected with a virus unless requested specifically by IDS to send to them for interrogation.
- Ensuring that antivirus/anti-spyware software is installed and maintained on any computer used to gain access to the University's IT facilities.
- Completing the mandatory Information Security Training as part of the University's Mandatory Training programme.

3.14 If any individual suspects that an email may contain a suspicious link, attachment, suspicious instructions, a threat or malicious request for financial payments, they should not reply to it, nor open any attachments, nor click on any links, nor make any payments and they must contact the IT Service Desk immediately for advice or log a call on the IT Service Desk.

https://servicedesk.keele.ac.uk

Email: it.service@keele.ac.uk

Phone: 01782 733838

3.15 Phishing attack emails should be reported as such to enable effective monitoring and prevention of further attacks. Guidance is available in the IT Service Desk Knowledge Portal

3.16 Users must be vigilant when using the University's email system. Malicious software and social engineering attacks are often delivered by email and can cause significant damage to the University's IT infrastructure as

well as reputational and financial damage. Be particularly cautious in relation to unsolicited emails from ANY sources. Information is available on IT Service Desk Knowledge Portal regarding issues such as phishing attacks and social engineering.

4. ETIQUETTE

4.1 Users are required to communicate in a professional and polite manner and consider how their reputation and that of the University may be affected by how they communicate and conduct themselves via online e-communications. Emails may be viewed as more formal and Instant Messaging (IM) as more informal, but polite and courteous language should always be used when contacting others.

4.2 Users should be mindful of 'spamming' others with multiple messages and emails. Consideration should be taken with the use of GIFs, images and emojis to avoid offence or upset to others.

4.3 Users should respect a person's online status. If a recipient is shown as offline, in a meeting, do not disturb, or out of office, sending an email instead of an Instant Message may be more productive and better appreciated.

4.4 The University encourages staff to leave their work at work and to resist responding to emails and messages sent to them outside of their normal working hours apart from in exceptional circumstances. Managers are also encouraged to set a good example by not sending emails and messages outside of their work hours to their staff wherever possible.

4.5 Many staff work flexible hours and therefore emails may be sent early or late in the day or even at weekends. Those who do should consider making a statement at the bottom of their email, such as:

"I work flexibly and sometimes send emails early/late in the day or at weekends. I do not expect you to read, respond or action this email outside your own normal working hours."
"Although I sometimes work outside of normal working hours, I don't expect you to reply to my email outside your working hours."

5. DATA PROTECTION GUIDANCE

5.1 Users should check the recipient(s) address(es) before pressing the send button—not only can it be embarrassing if a message is sent to the wrong person, it can also result in the unintentional disclosure of confidential information and / or personal data, which is the most common type of data breaches;

5.2 Before sending an email, especially those with attachments that may contain sensitive or personal identifiable information, users should consider whether additional safeguards are necessary such as encryption or direct sharing link provided if there is another way of communicating with the recipient. Where documents are password protected, passwords should be sent by alternate means; passwords should not be sent in the same or a following email.

5.3 When sending emails to a large list of recipients, especially if personal email addresses may be used, the BCC field should be used and not the TO or CC fields so as not to reveal personal email addresses to the other recipients. Failure to do so may lead to a breach of the DPA 2018/ UK GDPR and therefore may result in significant fines for the University and loss of reputation;

5.4 All emails, chat and instant messages are subject to Data Protection and Freedom of Information legislation and may therefore be disclosable to individuals upon request. Guidance on information requests can be found at www.keele.ac.uk/legalgovernancecompliance/legalandinformationcompliance/informationgovernance/accessinformationfromtheuniversity/;

5.5 If you do have personal information in your Keele email account, you should be aware that it may be audited as part of the monitoring described in Paragraph 3.9 and as part of Subject Access Requests.

5.6 When sending sensitive or highly confidential information via any e-communication method, ensure that this is marked as such and transmitted in an appropriately secure manner in line with the University Data Classification and Handling Policy. Always be mindful that written e-communication form part of University records and are subject to Subject Access Requests and Freedom of Information requests.

6. STAFF PERSONAL USE OF EMAIL

6.1 Although the email system is primarily for business use, the University understands that staff may occasionally need to send or receive personal emails while at work. It is expected, however, that staff use their personal email accounts in the first instance wherever possible. If working on campus, WiFi and standard internet access can be used to access your personal email systems and this should be the primary option as long as the access is appropriate.

6.2 Staff Keele email accounts must not be used to sign up to websites for personal use or subscriptions not related to work.

7. ROLES AND RESPONSIBILITIES

7.1 All members of the University are expected to promote and encourage compliance with the principles and spirit of this Code.

7.2 All users, as defined in paragraph 2.2.1, are required to abide by this policy and all associated guidance, processes and procedures aligned to this policy.

7.3 The CIO is responsible for reviewing and publishing this Policy and for providing policies, procedures, guidance, advice and training in support of it, and taking action pursuant to this Policy.

7.4 Directors or equivalent and Heads of School are responsible for ensuring that all staff and students within their area act in accordance with this Policy and established procedures

8. RELATED POLICIES AND PROCEDURES

8.1 The following Policies, Guidance and Procedures must be read in conjunction with this Code of Practice:

- IT Acceptable Use Policy

8.2 The following Policies, Guidance and Procedures should be read in support of this Policy. All policies are available in the Policy Zone :

- Data Classification and Handling Policy
- Data Protection Policy
- Information Governance Framework
- Information Security Policy
- Records Management Policy
- Records Retention Schedule
- Freedom of Information Act (FOI) Policy
- Monitoring and Interception Policy

9. REVIEW, APPROVAL AND PUBLICATION

9.1 The University will review formally the operation of this Code of Practice at least every three years, led by the Associate Director – Projects and Service Assurance (IDS), in consultation with key stakeholders across the University.

9.2 The University Executive Committee (or its sub-group) shall have final responsibility for approval of any changes to this Code of Practice, in accordance with the University Policy Framework.

9.3 The Code will be integrated into the annual student re-induction programme.

9.4 This Code will be available within the Policy Zone.

10. DOCUMENT CONTROL INFORMATION

Document Name	Use of Email Code of Practice
Owner	Simon Clements, Head of Projects and Service Assurance, Directorate of Information and Digital Services

Version Number	V1.0
Equality Analysis Form Submission Date	NA
Approval Date	27/February/2023
Approved By	University Executive Committee
Date of Commencement	27/February/2023
Date of Last Review	27/February/2023
Date for Next Review	27/February/2026
Related University Policy Documents	IT Acceptable Use Policy, Data Classification and Handling Policy, Data Protection Policy, Information Governance Framework, Information Security Policy, Records Management Policy, Records Retention Schedule, Freedom of Information Act (FOI) Policy, Monitoring and Interception Policy
For Office Use – Keywords for search function	