Internal Email (Staff-to-Staff) Use Policy and General Email Guidance for Staff

Introduction

Email is an expedient communication channel through which to send messages to colleagues at the University.

However, email has become increasingly burdensome, time consuming, less productive and less effective due to the very high volume of unnecessary and irrelevant emails staff receive daily. In many cases internal email is being used as the primary and sometimes only channel of communication; this is hindering the development of a collaborative and productive work environment that the University needs. The use of email as the default channel, is leading staff to adopt poor practices and behaviours. Therefore, the use of email for staff-to-staff communications, should be in line with the email policy below.

Any member of staff who is unsure about whether or not something they propose to do might breach this email guidance should seek advice from their Head of School / Service in the first instance.

This policy is designed to minimise the risks to the University from inappropriate internal staff-to-staff email use and to set constructive guidelines on the use of email at work for the smooth and efficient running of the business. Where something is not specifically covered in this policy or in the Guidance for Employees in Appendix One, and/or if there is anything in this policy that a member of staff considers to be unworkable or does not understand, advice should be sought from their Head of School / Service.

Policy

Staff **must only use** internal email to communicate with other staff in the University, for the following purposes:

- •   Urgent information circulation
- •   Formal communication of key decisions
- •   Transmission / dissemination of key documents (e.g. attachments)
- •   Logging of major concerns

For all other cases, staff are expected to seek to use more effective forms of communication including face-to-face meetings, telephone calls and on-line group working systems (e.g. Microsoft Teams).

Procedure

Staff must not engage in any negative or derogatory behaviours or poor practices set out in the General Email Guidance for Staff in Appendix One.

Staff who persistently breach this Internal Email Use Policy and General Email Guidance for Employees should be referred to the relevant Head of School / Service or senior line manager in the first instance, initially for informal coaching on effective email communications.

Persistent breaches should be reported to the relevant HR Business Partner and may lead to temporary suspension of email access and ultimately lead to formal disciplinary action.

Related Policies

- • Staff Acceptable Use Policy

- • Internet Security Policy

- • Harassment and Bullying Policy

General Email Guidance for Staff

1.0   Introduction

This is a simple guide to email use in the University. All staff are asked to adopt this guidance in order to enhance your communication, and lessen the risks to you and the University of poor email practices.

2.0   Legal Considerations

Email is a risky communications channel for sharing private or confidential information for a number of reasons:

The contents of emails are covered by:

- Data Protection Regulations,
- Defamation laws
- Freedom of Information Act
- Contract laws
- Copyright
- Wrongful discrimination laws

Individuals (staff, students, anyone) have a right to see any information that is written about them in an email whether University or personal email. They can request disclosure via a Subject Access Request to the University.

Under the legislation it is a criminal offence to alter, delete or destroy any information that has been requested by someone, in an attempt to prevent them from gaining access to it.

It is really important that you take care to keep the personal data you have access to, confidential. Under the Data Protection Regulations, individuals have a right to expect that their personal data is adequately protected by any organisation they have entrusted it to: there can be hefty fines (up to 10% of global turnover) imposed on the organisation for any serious breach, whether accidental or by neglect. A breach of confidentiality or loss of data would be classed as gross misconduct by the University.

Disclaimers included at the foot of an email may offer no legal defence.

Risky behaviours in emails

There are a number of common email behaviours which are either: irritating to the receiver and counterproductive; or increase the legal risks.

Always check factual accuracy of the content of an email before sending.

Whatever you write in an email about any living person, they have a right to see.

Be careful with email tone:

- Very negatively toned emails can sour relationships and reinforce entrenched positions.
- Never say things in an email that you wouldn't say to a person's face.
- Sarcasm, irony etc. are culturally specific and may not be read as intended and may be considered as rude or curt
- WRITING IN CAPITAL LETTERS IN AN EMAIL IS CONSIDERED THE EQUIVALENT OF SHOUTING AND BEING AGGRESSIVE. Avoid.
- Avoid sending angry emails when irritated or unhappy as invariably they can be counterproductive and can make the sender look foolish.

If you are on the point of sending, what could be perceived as, a very negative toned email, then write it and delay sending it for 12 or 24 hours. Then review it again and send only when you are sure the tone is right to elicit a helpful response. To avoid a mistake, always add the recipient email address last.

Avoid using "Reply all" and restrict the list of recipients to only those who are absolutely necessary, otherwise there is a danger of recipients receiving information that was not intended for them.

Only Carbon Copy (CC) emails to those who need to consider or take action as a result of its content.

Use "Blind CC" or "BCC" only to keep a circulation list of email recipients private for data protection reasons. Blind copying can otherwise contribute to a culture of mistrust and lack of ownership.

Be careful when including a long email trail in a reply or forward; they can increase the risks of some recipients receiving information that was not intended for them.

Include some of the original message for context, but be selective.

Don't use email to off-load your responsibilities - sometimes called "dumping". Always make sure the other party accepts the responsibility you wish to reassign or it may still rest with you.

Always make sure that any file attachment you are sending, that contains anyone's personal data, is encrypted. Do not send the password/encryption key to the recipient to the same email address; ideally you should use a different medium such as by telephone or private text message.

Remember that an email sent from your University account is similar to a letter on official University paper – do not say anything that might discredit the University or anything which might imply a legal obligation (unless you are authorised to do so). Your emails from your University email account reflect on the reputation of the University and may be interpreted as representing its views.

3.0   Good Email practice

Never use email for urgent matters. Regularly flagging messages as urgent creates an environment in which people feel they must view each email as it arrives. This creates an unpredictable and inefficient working day.

Giving the email a meaningful 'Subject' will improve the chances of it being read (and easier to locate later).

Restrict emails to one topic per message; send multiple messages if you have multiple subjects.

Keep messages brief and succinct. It may be read on the small screen of a mobile phone - long messages often don't get read beyond the first few sentences.

Use plain English and short sentences and avoid using acronyms or jargon, unless you are sure they are very familiar to the recipients of your message.

Proof read your message before sending.

When replying or forwarding with comments, include some of the original message for context, but be selective; don't reproduce the entire original email if it's a long one.

In your email signature, give your name, title, contact details and web address. There are further guidelines for Email sign-offs within the University's corporate guidelines.

Avoid using backgrounds in emails- they increase the size of messages and can make a message display incorrectly or be unreadable for people with visual impairments.

Explain if you expect the recipient(s) of your email to do something as a result of your message. For example, do not just forward a message onto someone and assume that they will know what you expect them to do with it.

Do not attach large files to emails if you could use a link to a shared network space or a website instead. Most email servers will reject emails with attachments over 12mb – sometimes smaller than that.

Out of hours home and mobile access to email is provided for your convenience, but please respect others private time and remember you should have no expectation of receiving a response to your messages outside of normal office hours.

In order to ensure we follow appropriate environmental and sustainable behaviours avoid and minimise the printing of hard copy email correspondence and/or attachments.

4.0 Receiving emails

Beware of Phishing emails - never reply to emails asking you to provide your login and password details beware of clicking on weblinks in an email unless you are confident about its legitimacy. The IT Service will never ask you for your password, and any message that requests this is a malicious scam.

Delete junk or spam emails or forward to spam@bolton.ac.uk if they look malicious. Do not open any attachments or click on any links in these messages.

When you are away from the office and not picking up emails, set an 'out of office' reply giving an alternative contact for any urgent queries.

Do not forward any chain emails, scams or hoaxes.

TITLE OF DOCUMENT: Guidance for Employees	Internal Email Use Policy and General Email
Policy Ref	
Version Number	1
Version Date	March 2020
Name of Developer/Reviewer	Chris McClelland
Policy Owner (Group/Centre/Unit)	Human Resources
Postholder responsible for implementation	Executive Director of HR
Approving Committee/Board	Executive Board
Date Approved	
Effective from	
Dissemination method (eg website)	Website
Review Frequency	Every 5 years
Reviewing Committee	Executive Board
Consultation history (individuals/group consulted and dates)	
Document History (e.g. rationale for and dates of previous amendments)	