Information Governance

Email Good Practice Guide

Protecting personal and confidential information is vital to ensure both you and the University comply with current legislation. Due to the lack of control of emails, it is best practise not to send email that contains sensitive information, if it can be avoided.

Email is not secure and the privacy of a message cannot be guaranteed. The message may be forwarded, printed or permanently stored by the recipient. Do not put anything in an email message that you would not want to be read by everybody.

Email is a key tool at Loughborough University allowing for quick and efficient communications. This document outlines best practices to minimise potential risks associated with email. Before sending any email consider if it is the best form of communication or whether a visit, phone call or even a letter might be more effective.

Always give your email a descriptive subject

Well-written subject lines allow the recipient to quickly find your message and prepare for its content. Indeed a good subject line may sometimes constitute the entire message

Put an expiry date on time-specific email

If you send a time-specific email, add an expiry date so the email automatically disappears when no longer relevant. When returning from holidays or similar it can be frustrating to see many emails related to events that have passed.

Requests under the Freedom of Information (FOI) Act

It is a legal requirement that all FOI requests are answered within 20 days. Each user is responsible for checking for such requests and forwarding any received to foi@lboro.ac.uk.

Emails are quick and convenient but not secure. It's easy to fake email addresses

Faking email addresses (‘spoofing’) is easy. An email ‘from Bill Gates’ could actually be from anyone. Equally it is not possible to prevent people sending emails that appear to come from your account. This does not mean your account has been compromised. Conversely any email you send may be readable by others. Think of emails as being as public as postcards. Any email that asks for your bank details, password or security details is fake – delete it.

Emails persist forever – think very hard before pressing send

Every single email sent and received by the University email system is liable to be archived and may be retained for years. An angry email you send in haste could come back to haunt you later. Good advice might be to write the message while angry, but not to send it until later when you are calm. It is strictly against University rules to use email to abuse, bully or harass anyone and these terms will be interpreted by others if upset is caused. Under the Data Protection Act anyone has the right to request access to any email about them and such requests may be granted by the University.

Send emails only to those people who really need to see them

Target your messages to the minimum number of people necessary. Emails should be sent 'To' people who need to do something and 'CC-ed' to people who need to be aware. Avoid sending requests 'To' more than one person. This is likely to lead to wasted work as each recipient tries to deal with the contents of your message.

Don't be accused of sending spam, either externally or internally

Be careful when sending email surveys; the recipient must not perceive your message as spam. Contact the IT Service Desk for advice on sending email surveys or questionnaires. Never forward virus warnings or similar to others without checking first with the Helpdesk; usually such warnings are fake. Internally, be careful sending 'thank you' messages; busy recipients may just see them as 'Inbox filler'.

Don't invite spam

Unwanted "spam‟ email is a problem the world over. Make sure you aren't inviting spam, in particular:

- Never reply to spam, you will only get more of it ('out of office' messages/rules have the same effect, so should be used sparingly)
- Create a personal email address (see below) and use this whenever you sign up for a service. Only use your University email address when you trust the other party.

Phishing Emails:

Phishing is a way for scammers/hackers to steal your identity to gain access to your usernames and passwords. Phishing usually originates through spam emails. These emails look like they have come from genuine companies or from people you know asking you to update your details or wanting to share something with you. The following highlights signs to spot phishing emails:

- The senders email or web address is different to the genuine organisation's address;
- The email is sent from a completely different address;
- The email doesn't use your real name. but uses a generic greeting such as "Dear Customer";
- The email threaten that accounts may be disabled unless action is taken;
- You're asked for personal information such as usernames, passwords or bank details;
- The email contains spelling and grammatical errors;
- The email contains links to bogus websites;

Use a personal address for personal email

The email system is legally the property of the University, which allows it wide-ranging rights to access mail as part of an official investigation, such as Bullying and Harassment or Health and Safety. While there is no problem with the account being used to send limited amounts of personal email, there is little need as it only takes a few seconds to create a free account with a provider such as Hotmail, Google or Yahoo. These accounts will continue to work should you leave the University. Personal mail accounts should always be accessed using web interfaces to avoid possible problems of having multiple mail clients on your work computer. All University business, however, must be conducted using either your Loughborough University email address.

Never send photographs, music or video by email

Media files such as photos, music or videos can be very large and can cause a range of problems for both the sender and intended recipient. Please contact IT Services on advice about sending large files

Be aware of what happens to your email account when you leave

Email accounts are deleted shortly after a staff member leaves and are irretrievable. Prior to deletion other staff may have access to the account to ensure messages are, or have been, dealt with. It is the departing staff member's responsibility to delete any private messages before they leave if they wish to ensure these are not potentially seen by other staff.

Avoid using person-specific addresses in brochures and promotional or support material

Where there is a valid business case, IT Services are able to create generic email addresses such as infogov@lboro.ac.uk.

Always save email attachments before working on them

You may often receive documents via email on which you need to work. Always save these to your workspace before working on them to prevent the risk of your work being lost.