Guidelines for sending bulk email

What is bulk email?

Bulk email can be an efficient way of communicating information to many people – for example instructing recipients to visit a website or online system. A bulk email is any email sent to multiple recipients. It could be to a small group of individuals or can be as large as the whole of the student body. It can be an email sent internally or externally.

Please note that this guidance is intended for individuals using Outlook as their primary method of sending bulk emails.

Where there is a recommended email mass mailer software to use, this can be used to send out emails, for example My Aberdeen has a function by which all students on a particular course can be emailed safely. Please contact the Service Desk for more information.

When sending emails to a number of people, there is a significant risk of erroneously sharing personal data and committing a data breach. This could result in financial and reputational consequences for the University. Please see the 'Data Protection Breaches' box below for further information. For this reason, it is important that you take care over sending emails to multiple recipients and ensure that you follow these Guidelines.

Additionally, the characteristics of bulk emails mean they are often mistaken for phishing scams[1]. This means that mail filters may direct your legitimate email straight to recipients' Junk Email folders; or that your recipients suspect your email is a phishing scam and delete it.

The aim of these Guidelines is to help you prepare bulk emails that achieve a balance between ease of use and reassurance for recipients, as well as lowering the risk of inadvertently sharing personal data. Therefore, please follow the steps outlined below.

When composing a bulk email:

If your email contains personal sensitive data, and you do not wish to disclose the email addresses of recipients to each other, read Steps 1-4 if not move to Step 5:

Examples may include:

- If you are writing out to all students receiving a counselling service, you must not disclose the identities of the individuals receiving a service as part of the bulk email.
- If you are writing to a membership list for a conference, you should not disclose the email addresses of the recipients if this is not usually shared with them.

1. If your email contains any personal information, you will need to "blind copy" the recipients – this function hides the individual email addresses from all recipients. Please see further information in the box below.

[1] See also our user guides for help with 'Protecting yourself from Phishing Scams' and 'Dealing with Junk Mail and SPAM'.

How do I set up the blind copy BCC option?

When composing a message, switch to the Options tab > Show Fields group and press the Show BCC button. Add the recipient's name(s) to the Bcc box in the usual way, i.e. either by typing or selecting from the Address Book. From now on you will always see the blind copy Bcc box when composing an email.

2. You can also remove Auto-complete from your Outlook and this is recommended best practice. Auto complete will suggest names when typing into the To, Cc and Bcc lines. This can lead to incorrect email addresses being added by mistake.
3. If sending bulk emails to colleagues and students, always use the Outlook Global address list, which will allow you to check that you are sending the email to the correct person.
4. **Stop and check before sending!** A pause to check the email can make the difference between committing a data protection breach and sending an email safely.

Data Protection Breaches

The Information Commissioner's Office fined HIV Scotland £10,000 following a breach of data protection law as a result of an email being sent to 105 people which included patient advocates representing people living in Scotland with HIV. All the email addresses were visible to all recipients, and sixty-five of the addresses identified people by name. From the personal data disclosed, an assumption could be made about individuals' HIV status or risk.

Whilst the aim of these Guidelines is to reduce the likelihood of a breach occurring, if a breach occurs, it is vital that all staff report a personal data breach, however minor, promptly after discovery. They can be reported to the Data Protection Officer (dpa@abdn.ac.uk). You can also call the Information Governance Team if you wish to discuss a breach or whether an incident is a personal data breach on
01224 27(3175), 27(3079).

Bulk email guidelines:

5. Use identifying information to make it clear that the email comes from the University of Aberdeen
   - Include a high-resolution University logo.
   - Use a abdn.ac.uk email address
6. Provide a detailed explanation of why you are sending the email. Phishing emails by comparison are often vague about their purpose – '*We need you to verify your details*,' for example.
7. Double check your email carefully for grammatical errors and spelling mistakes before you send it out. Phishing emails commonly contain such errors.
8. **Never** ask recipients to supply sensitive information (such as username/password, bank details, PIN numbers) by replying to the email, or completing a document and sending it back. It is also recommended that you avoid asking recipients to click on a link and fill in an online form. If this cannot be avoided, then please follow Step 9 below.

9. It is preferable not to include any links, but if you must:

    - Write all links out in full, using https not http, e.g. https://www.abdn.ac.uk not University website.
    - Avoid using deep or complex links, such as: https://www.abdn.ac.uk/staffnet/documents/policy-zone-information-policies/DIT_cond-IT.pdf

    Note: You may not be able to follow this advice if links are unique to recipients – links to an online survey, for example. If this is the case, try to ensure that nothing else about your email makes it looks like phishing.

10. If you need recipients to go to a web page to log in to a system, instead of including a direct login link, describe the simplest way to navigate to the page.

    - For example: ‘Go to **StaffNet** and select **Outlook Web Access** from the **Quick Links** section’ instead of ‘*Login to Outlook Web Access*.’

11. Do not attach documents to your email. Instead, ask recipients to download documents from the University website, describing the simplest way to navigate to the document location.

    - For example: ‘Download our **Self Certification Form** from the **Holidays, Leave and Absence** section of StaffNet.’

12. Provide a way for recipients to check that your email is genuine.

    - Name an individual or team whose contact details are available in Outlook’s address book or can be validated on University website. This allows a recipient to get in touch by other means.
    - Refer recipients to the University website for further information to help validate your message, e.g., ‘*Search for **TaD Team** on the main University website.’*

13. The University has email security measures in place to protect us from bulk external emails. Bulk email from untrusted external senders may be moved to junk, tagged as spam, or potentially rejected entirely. If you are using an external service to bulk email the University, then you must contact the IT Service Desk for advice in advance of the service going live.

Help and Support

Contact the IT Service Desk at myit.abdn.ac.uk or contact dpa@abdn.ac.uk for help and support.