**Key message: Double check at the risky points**.

1. **Adding information**
2. Can you minimise the personal/confidential data as much as possible?
3. Can it be fully anonymised?
4. Can we replace names with pseudonyms or initials? Can we just refer to “their child”?
5. Consider data minimisation – do we need to send the full file, or can we just send an extract?
6. When adding attachments – is it the correct attachment, and correct content (be careful with spreadsheets and extra tabs/worksheets)
7. Save all templates as Template files (eg .dotx / .xltx) to prevent them from being over-written
8. Ensure a sensible file naming convention is in place and followed by everyone
9. Send a link rather than attaching the actual document? (to reduce duplication)
10. Collaborating? Share it in MS Teams/SharePoint rather than emailing to prevent multiple versions of the same file
11. **Entering** email addresses:
12. Can you reply to a previous email? If not get them to send you a quick email
13. When selecting from address book – ensure you select the correct recipient? 2 x Sarah Smith – check the properties/details of which department they work in
14. When selecting from autofill be very careful – you can delete old/obsolete addresses by clicking X (far right) when they come up after typing the first few letters of their name/address
15. When using a distribution list - expand the list by clicking on the + button (see example:) and check for accuracy
16. When **emailing to multiple external recipients** (i.e. parents) – Ensure to use blind carbon copy (BCC) - which is available in the Options tab when drafting an email, simply email yourself and BCC the external recipients (each will get an email without revealing the others email addresses).
17. When **receiving emails** which ask you to click a link, open an attachment, or reply regarding financial transactions – if unsure as to the validity check with the IT/DPO if you’re unsure. Consider the following:
18. Does the email look and feel right?
19. Does it address you in person?
20. Is there poor grammar/spelling?
21. Was I expecting it? If not, contact the other person by other trusted means (e.g. SMS, phone call) to verify
22. Just because it looks like it’s come from a genuine email address, email addresses can be spoofed/masked
23. Is it asking you to bypass internal controls and to ‘send urgent payment’? These emails sometimes ‘appear’ like they come from inside the organisation and from senior management.
24. When **clicking send** - Consider setting up an email sending delay. This provides a safety net whereby after clicking *Send* the email sits in Outbox for a set amount of time before it actually delivers (set it yourself – we’ve set ours to 1min) Obviously this only helps if you quickly realise an error and can then intercept it in Outbox.
25. When **sending sensitive content** – Consider encrypting the data either using a secure email tool (such as Egress, or Office365 Message Encryption (OME)). Or encrypt the data in a MS Word document (File/Info/Protect - but ensure you encrypt a copy and not the master!). Then attach in an email and communicate the password by other trusted means (e.g. SMS/Phone Call/Pre-agreeing it – such as the pupil’s DoB in DDMMYYY format) and not by email!