

# Stop, Think, Check

## Take a moment

Did you know that one of the most common reasons given by staff for an information security incident is 'human error'?

We are all very busy and are trying to juggle competing priorities, but by taking a step back and checking that everything is correct before clicking send on an email or sealing a letter could prevent us causing a breach of someone's personal or sensitive information and a potential fine from the Information Commissioner's Office (ICO).

Let's look at the types of common security incidents and how to we can avoid them:

**Wrong recipients** - This is by far the biggest cause of information security incidents - wrong e-mail address, wrong address on envelope, wrong document attached or in an envelope, additional worksheets in an excel spreadsheet, and even information being disclosed to the wrong person verbally.

Ensure you have the intended recipient on your email or envelope, correctly spelt and addressed. Once in the postal system we have no control of the letter if it goes to the wrong recipient or is not delivered. It is worth considering if you really do need to use post and whether other means could be used instead e.g. e-mail or hand delivered.

Take particular care where there are recipients with the same name, often in emails distinguished by just a number or letter difference. Check the document is correct before sharing.

Always be careful of who you are talking to - make sure they are who they say they are and be careful about what you tell them, and never discuss clients or OCC business in public - you never know who is sat behind you on the bus!

**Emailing securely** - Personal and sensitive information sent outside of the organisation must be sent securely, and this may mean using a secure email method (e.g. Egress). If you correspond with a private email (e.g. Hotmail) you must use the designated secure email method unless the recipient is happy to receive open email.

**Auto Complete** - many email issues result from Outlook's clever Auto Complete function, which tries to pre-empt which email recipient you want. An example of this is where a member of the public has been emailed to their personal address and this can be 'remembered' by the email system. When entering a similar name in Outlook, Auto Complete may offer this personal address rather than the intended address, and personal and sensitive information could inadvertently be sent outside of the organisation and out of our control.

Check which email has been selected before sending, or you can turn Auto Complete off. The extra seconds taken to look up contacts in the directory or your address book is nowhere near as long as the incident investigation process!

**Need to know and CC all** - consider whether everyone on the mailing list or at CC needs to know this information or even see the other recipient's email addresses. Emails containing personal and sensitive information should be restricted to only those who need to know. Always use BCC where appropriate to hide the email addresses of the other recipients.

Consider whether email is the most appropriate method of communicating this information as there may be other more targeted systems available.

**Don't click that!** - remember, phishing emails and scams are a constant threat. If you don't know or trust an email sender or the content, do not click. Report it to the OCC ICT Service Desk

Don't forget that you have an important role in the prevention of information security incidents, and you are the last line of defense.

**Act fast**

If you become aware of any potential information security incidents, whether you have done this yourself, or you know that someone else has, notify the Information Management team straight away either by email or the online form.