



Phishers can use publicly available information about you to make their emails look genuine. Review your privacy settings on social media and be mindful of what you post there. Ensure you check the address that an email has come from. Phishing emails can appear genuine but they are actually fake. They might try and trick you into revealing sensitive information or contain links to a malicious website or contain an infected attachment. Anybody can click on a phishing email in error. If you think you have done this, tell a member of staff immediately. Get to know your college's policies and processes to make it easier to spot when something does not look quite right. Click [here](#) to see more.

Common features of a phishing email that may look genuine can include poor quality images of company logos, spelling or grammatical errors, addresses you generically rather by your name, urging you to take immediate action.

### Message Content

Be mindful of what you are writing. If an individual makes a request under the General Data Protection Regulations (GDPR) rules, they have the right to request any information and organisation holds on them. Often, this will include emails or notes made in a meeting. Even emails that are labelled "Private" or "Confidential" can be disclosed in some cases.

Things to consider in your communication:

Keep it factual and objective. Don't be subjective or critical of an individual

Before clicking "Send", double check you have the right email addresses and that it's going the right people. Once it's gone, it's very hard to retrieve it

If you're sending a group email, consider using the Bcc option if there are external or personal email addresses being used

Be clear to the recipient if your message is confidential or whether it should/should not be forwarded onto others

Ensure the title of the email is relevant to the contents and do not include personal data

Send your email to the recipients that need to receive it. Be mindful of the "Reply to all" functionality

Password protect any attachments that contains sensitive information and send the password via a different channel (verbally or text message for example)

Consider other options for sharing sensitive information. One example could be OneDrive or other cloud sharing services

Don't save emails that contain personal data. Once the personal data has been retrieved and stored safely, delete the email. Remember to do the same with your Sent items too

If you find yourself regularly sharing documents with the same individual(s), consider using OneDrive or Teams

If you have any questions about e-mail security or transmitting personal data securely, contact the Data Protection Team via [dpo@ncgrp.co.uk](mailto:dpo@ncgrp.co.uk)



### Password Protect

If you are going to be sending information to others via email that contains personal data or sensitive information, make sure you password protect it. (File – Protect Document – Encrypt with Password – Set password)

If password protecting a document, advise the recipient of the password using a different method. Don't put the password in the same email as the attachment. Send a subsequent email, advise verbally or via text message.

There are things to consider when making up a password, either for a document or for system access. These include:

- Make your passwords strong and memorable. For example, use 3 random words and make that your password
- Try to use different passwords for anything work related to any passwords you may have created for personal use
- If you need to write down your passwords, make sure they are stored somewhere safe and secure

Click [here](#) to find out how.



### Use of NCG Systems

Any NCG device that you use can be exploited both remotely and physically but you can protect them from many common attacks.

Don't ignore software updates. They will contain patches that will keep your device secure.

Always lock your device when you are not using it. Use a pin or a password to protect it.

Only download apps from trusted sources like Google Play or the Apple Store. Do not download apps from unknown or untrusted sources.

Try to ensure that any work you do is done on NCG devices and not downloaded on personal devices. You should also avoid sending any business related or personal data to your personal email address.

**Be protected**


If you are using a personal device to do your work on, make sure that the device is as safe and as secure as possible to use. Always install any required software updates. Click [here](#) for more information.



**Office 365**

Office 365 is a suite of desktop apps that include ones that you are familiar with like Word, Excel and PowerPoint.

You should try and use Office 365 wherever possible. Doing so will avoid you having to download documents to your personal devices and means that you will have access to your documents from wherever you are.



**Remove data**

If it is unavoidable to download personal data to a personal device, ensure that this data is removed at the earliest possible opportunity once you have used the personal data for its given purpose.



### Report breaches

Reporting cyber incidents promptly to either your line manager or a member of staff is key. Taking quick action will reduce the harm caused by cyber incidents.

Cyber incidents can be difficult to spot, so don't hesitate to ask for support or guidance if something doesn't feel quite right. Don't leave it to someone else to report a potential breach. Take ownership and report it as soon as possible. Even if you have clicked on a link that you should not have, please report it. Click [here](#) to find out what a Personal Data Breach is.

If you think there has been a cyber security breach or incident, please make sure you report it as soon as possible to [dpo@ncgrp.co.uk](mailto:dpo@ncgrp.co.uk).