Data Security – FAQS

Do the College Data Protection related policies and procedures apply if I am working at home?

Yes. The College remains Data Controller for the processing of personal data as per GDPR and the Data Protection Act (2018). While we have moved 'on-line', the appropriate data protection guidance remain operational.

Policies and procedures are available on the staff intranet:

https://staff.nrc.ac.uk/policy-procedures/Pages/informationGovernance.aspx

I don't have a College PC or laptop. Can I use my home computer?

Yes, however you should avoid downloading personal data to your home computer. If there are occasions where you need to download, you must delete as soon as the work activity has been completed.

Staff should observe the following guidance when using personal devices:

- Make sure all latest updates have been run on your device to enhance security.
- Use Microsoft Office 365.
- Send information via One Drive or links to SharePoint (useful guidance)
- Do not use your personal email addresses for College related activity. We cannot stand over the security of these providers.
- Do not use your College email address for personal activity such as online shopping etc.
- Log out of your College account before letting family members use the device.
- Continue to be on your guard for phishing emails.

Useful guidance

- **5 things to watch out for**: https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email
- **NCSC - Phishing attacks: dealing with suspicious emails and messages** - https://www.ncsc.gov.uk/guidance/suspicious-email-actions
- **JISC** - https://www.jisc.ac.uk/blog/coronavirus-scams-how-to-spot-them-16-mar-2020
- **NCSC** - https://www.ncsc.gov.uk/news/cyber-experts-step-criminals-exploit-coronavirus

NOTE: Remember this applies to personal emails as well.

What software can I use?

Staff should only be conducting College business on College approved platforms e.g. Microsoft 365, Canvas, Learning Assistant. Staff should not use unapproved software for any College related activity e.g. Zoom (free version), WhatsApp, Google Classroom.

Can I record on-line sessions (lecture capture and business meetings)?

Not all sessions need to be recorded.

In terms of teaching, recordings can be made when the session is intended for reflective learning, for assessment purposes or to permit flexibility for the benefit of students who may not be able to attend during the timetabled session.

In terms of corporate activity, recordings should only be carried out for the purpose for the note taker and non-attendees.

Notifying attendee of recording:

- Students/staff have been issued with a Privacy Notice providing them with an expectation of how their information will be processed. Staff must not use recordings beyond these expectations.
- Attendees must at all times be reminded in advance that a session is being recorded.
- You may wish to remind them of items which could be caught on camera in the background of their home environment e.g. pictures etc.

Managing the recording

- Recording should only take place after cameras/microphones have been disabled of those who do not wish their data to be recorded.
- Monitor the Attendee List to ensure only expected participants are present

The following are relevant features of Teams regarding privacy and safeguarding:

- Any attendee from inside the host organisation can start or stop a recording. This feature is not available to guests from external agencies or anonymous attendees.
- All internal attendees can replay the recording.
- External guests cannot replay recordings.
- Recordings are securely stored on Microsoft's Stream cloud platform.
- Be aware not to accidentally share the Teams screen within the current meeting session, as your private chat/files could be visible, and this may constitute a breach.

How should I communicate with students

The College has approved software to allow staff to communicate with students:

- Canvas
    - Allows messages
- City & Guilds Learning Assistant

    - Allows messages
- Tribal EBS
    - Allows tutors to send texts/emails to class groups
- Outlook
    - Email only

Should you find it necessary to contact a student using your mobile phone (College or personal), then you must only ring them including the prefix 141 to hide your caller ID e.g (141) 0777777777 or (141) 028111111.

The College does not endorse using the following platforms for contacting students:

- WhatsApp
- Zoom (free version)
- Closed social media groups
- Other unauthorised platforms to communicate with students.

What can I do to protect hard copy data?

- Where possible avoid printing information containing personal data. If this is unavoidable, you must shred documents once you have finished with them. **Under no circumstances should personal data be put into your household bins. These are not secure**.
- These documents should be protected from view from other members of your household with appropriate security applied to them.
- Keep a record of hard copy information you have removed from the College prior to closure and communicate this to your line manager.

What else can I do to safeguard information?

Conversations:

Staff are asked to be mindful of their surroundings when having either telephone/online conversations where personal information is being discussed. Many staff may have "smart speakers", such as Amazon Alexa, Echo, Google Home, located in various rooms within their house, and the unpredictable recording facility on these devices these may have data privacy implications for College information.

Staff are asked to be mindful of the location and activation of these types of devices when conducting College business from home, such as discussing personal data on the telephone.

Photo fun:

You may want to share pictures with family and friends of your 'world of home working' however always be mindful of what information you are sharing and which could inadvertently be made public. Examples of things to avoid sharing:

- documents/emails/images on your screen which identify individuals (you could display the College website homepage as it is in the public domain).

- papers with personal data on them.
- diaries with your list for the day which may contain personal data.