UST
University Schools Trust

GDPR AND DATA PROTECTION:
GUIDANCE REGARDING REMOTE ACCESS / WORKING AT HOME

Please note: this guidance is not intended to be used in general circumstances. It is solely for the purpose of supporting our schools during the specific exceptional circumstance of the coronavirus outbreak.

Following the announcement by both the Prime Minister, Boris Johnson, and the Education Secretary, Gavin Williamson, all schools in England will close from Friday 20th March until further notice for all pupils except children of key workers and the most vulnerable.

As a consequence, it is expected that the majority of staff will need to work from home. Although this will be a hugely challenging situation for us all, it is vital that we maintain GDPR compliance to the best of our ability.

School devices
In the first instance, where possible, all staff should only use school devices. School devices should already be secure with the appropriate encryption and security.

Remote access via a virtual desktop
These systems should already be secure and will enable staff to save any documents to the school network and not the device they are using.

Remote access via One Drive/Google
If staff use their own device, there is a risk that any data produced and saved will be stored on their own device automatically. This is not GDPR complaint. Therefore, it is required that the following measures are undertaken:

- If using a desktop/laptop, create a new user account on the device, which can be password protected.
- Create a specific folder in this account for downloads or documents created.
- All documents are uploaded to the One Drive/Google account as soon as completed.
- The folder should be cleared, and all items deleted as soon as possible.
- The recycle bin/deleted folder also must be accessed and the contents deleted.

Mobile/iPad

- These devices must be protected via PIN/password/fingerprint.
- These devices can be used to access emails etc. but it is important to be aware that any document attachments accessed will downloaded to the device.
- Documents, therefore, should be viewed and not downloaded to minimise the risk.

Surroundings

- When discussing students via telephone, staff must ensure that conversations are held in private - away from family members.
- Staff must ensure the device they are using is kept safe.
- Staff must continue to 'lock' the device when they are not using it.

Breaches

- Any breaches of data should continue to be reported in the same way and staff should be reminded that, if significant, we will still need to report within 72 hours.