There has been lots of useful and helpful information circulating in the past couple of weeks in relation to working remotely. What we attempt to do here is highlight the most important points for school staff to consider when working remotely.

A well-thought-through approach will make changing to remote working a smoother process.

Teleconferencing and videoconferencing

Teleconferencing and videoconferencing is a valuable tool for keeping in touch with staff and also of course for delivering distance learning. At a minimum, teleconferencing facilities should be set up and tested initially with staff. Teleconferencing facilities are preferred generally as they can be accessed via smartphones and therefore are for staff and students who may not have a dedicated workspace at home, or who have to share a device.

Students should be reminded that the same rules apply as in the classroom. The school code of behaviour and the school discipline rules will still apply. Good etiquette and good manners are still expected.

Appropriate dress code is also expected by all participants in a video call.

Possible providers include Zoom, Blue Jeans, MS Teams, or Google Hangouts.

Devices

- Take extra care that devices, such as USBs, phones, laptops, or tablets, are not lost or misplaced,
- Make sure that any device has the necessary updates, such as operating system updates (like iOS or android) and software/antivirus updates.
- Ensure your computer, laptop, or device, is used in a safe location, for example where you can keep sight of it and minimise who else can view the screen, particularly if working with sensitive personal data.
- Lock your device if you do have to leave it unattended for any reason.
- Make sure your devices are turned off, locked, or stored carefully when not in use.
- Use effective access controls (such as multi-factor authentication and strong passwords) and, where available, encryption to restrict access to the device, and to reduce the risk if a device is stolen or misplaced.
- When a device is lost or stolen, you should take steps immediately to ensure a remote memory wipe, where possible.

Emails

- Use school email accounts rather than personal ones for work-related emails involving personal data. If you have to use personal email, make sure contents and attachments are encrypted and avoid using personal or confidential data in subject lines.
- Before sending an email, ensure you're sending it to the correct recipient, particularly for emails involving large amounts of personal data or sensitive personal data.

Cloud and Network Access

- Where possible only use the school's trusted networks or cloud services, and complying with any school rules and procedures about cloud or network access, login and, data sharing.
- If you are working without cloud or network access, ensure any locally stored data is adequately backed up in a secure manner.

Paper Records

- It's important to remember that data protection applies to not only electronically stored or processed data, but also personal data in manual form (such as paper records) where it is, or is intended to be, part of filing system.
- Where you are working remotely with paper records, take steps to ensure the security and confidentiality of these records, such as by keeping them locked in a filing cabinet or drawer when not in use, disposing of them securely (e.g. shredding) when no longer needed, and making sure they are not left somewhere where they could be misplaced or stolen.
- If you're dealing with records that contain special categories of personal data (e.g. health data) you should take extra care to ensure their security and confidentiality, and only remove such records from a secure location where it is strictly necessary carry out your work.
- Where possible, you should keep a written record of which records and files have been taken home, in order to maintain good data access and governance practices.

General advice and security

1. **General:** You need to be realistic about what can be achieved with technology given people's existing capabilities and skills.
2. **Fraud / phishing:** Attempts are unfortunately on the increase.
3. **Physical security:** Even when working from home, PCs and laptops should have two step password protection - involving both a password and a pin number sent to your mobile phone.
4. **Privacy:** Individuals are potentially more vulnerable to having their privacy rights exploited when their image and voice is being beamed remotely over the web. *Students must be reminded that the use of mobile phones or other devices to*

photograph or record staff or other students for the purposes of publication elsewhere is strictly prohibited and in breach of those individuals' basic human right to privacy.

Schools should also communicate with parents that they need to satisfy themselves that they are comfortable with their child's use of distant learning platforms from a privacy perspective. Parents should be aware that their child is in video communication with their teachers and SNAs and ensure they are comfortable with how these communications are being conducted.

5. **Email:** To avoid data breaches, extra security precautions need to be taken in relation to the content of emails.
6. **Online file sharing:** Online file-sharing services may not be secure enough for sensitive and confidential communications. All large files or data sets should be sent using applications that provide a number of security features, including:
    - Encryption,
    - Link-expiry settings,
    - Number of allowed downloads, and
    - Password protection.
7. **Downloading Applications:** School staff need to satisfy themselves on their GDPR obligations in the use of all products, in the normal manner. We would caution against use of apps that have not been assessed as GDPR compliant.