Protecting personal data when working remotely

As we all embrace these new ways of working (predominantly remotely) we thought it was prudent to provide some guidance on safer working practices regarding data privacy and security.
Below are some tips that you should follow to ensure that personal data is safe when working away from your regular place of work.

Laptops, tablets, mobiles, androids, smart phones, USBs, etc.

- Take extra care to ensure that your equipment is not lost, stolen or misplaced
- Ensure you use your equipment in a safe location especially if you share your accommodation with others
- Use screen protectors and be vigilant about who else can view the screen especially if you are working on Special Category data, e.g. health data of employees
- Lock your computer, laptop, etc. if you do have to leave it unattended for any reason
- Make sure your equipment is turned off, locked, and stored carefully when not in use
- Use effective access controls, password protection, and ensure your equipment has encryption to restrict access to the device, and to reduce the risk if a device is stolen, lost or misplaced
- When a device is lost, stolen or misplaced, you should take steps immediately to report this so that appropriate security measures can be taken
- Make sure that your equipment has the necessary updates, such as operating system updates and software/antivirus updates. Speak to your IT support and Security team if you have any doubts.
- Use only school provided devices. If you need to use a personal device, always ensure that this has been reported and has the necessary security added
- Ensure that you have the correct power pack
- Never connect a personal device to your school provided device even for charging via a USB port – once connected it becomes a highway for data and/or viruses to be exchanged

Emails

- Use work provided email accounts and not personal ones for all work-related emails. If you have to send information to a personal email address make sure contents and attachments are encrypted, i.e. mark the email as “Confidential”. Attachments should be password protected. Avoid using personal or other confidential data as the subject of the email.
- 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. Look out for auto-complete and be vigilant that this is the correct addressee.
Working in the cloud using Microsoft O365 and Google e.g. conference calls and Teams Meetings

- Use work provided cloud accounts and not personal ones for all work-related business.
- Ensure all staff required to work in the cloud remotely have received appropriate training to enable the use of technology. Make sure that staff are aware of their log in details and can log in successfully.
- Ensure staff have been allocated to appropriate cloud working groups and have appropriate permissions set to access information.
- Make sure staff are aware of which staff members are on the call either through audio and/or video connection to avoid over-sharing of information or unauthorised disclosures of information. Staff should also know how to disable the camera and/or microphone when needed.
- Make sure that you terminate all calls correctly at the end of a meeting to disconnect from the individual or group call.
- Remember that someone could overhear your conversations. Use headphones where possible to ensure that the person speaking is not broadcasting to the household. Close the door if you work in a separate room and be vigilant about who may overhear your conversations.
- Secure your own personal information if using video conference calls – check what can be seen behind you when you are using video conferencing.
- Don’t discuss anything personal if possible.
- Don’t record any Team Meetings or Conference calls unless all participants are aware that it is being recorded – delete footage/recordings when no longer required.

Phone Calls

- Pay attention to what you say on the phone if you are in a public area.
- Do not use personal devices to make contact with parents/carers to avoid sharing your personal contact details.
- Be aware of information exchanged via texts and remove/delete from your phone when no longer required.

Paper Copies

- Restrict the use of paper to a minimum and if you must have paper copies, always keep them secure and locked away when they are not in use.
- If you are printing remotely and other people have access to the printer, please ensure you take the copies off immediately.
- Destroy copies in a safe and secure way and do not put papers in the household waste.
For more support on data protection for your school, please email edtech@entrust-ed.co.uk and we will arrange a virtual conversation, free of charge.