Data Protection DOs and DON'Ts Home Working

Staff may be asked to work from home on occasion, for whatever reason be it a national disease or the concrete used in your schools, but protecting children and staff data must remain a highest priority. It is known that the risks for data breaches become much higher when data is accessed remotely or on a portable device and must be considered. With simple planning and by applying common sense you will help reduce these risks greatly.

Here's a few tips which are also explained on a video. Click here to view

You cannot share a device unless there is strict access control to personal data you use from school.

This will include:

- school emails
- learning platforms
- your electronic mark-book
- administration systems such as SIMS
- …and many other systems

DO

- Be vigilant – no-one else in your household must have access to or see the data you are using and you must be sure you use strong passwords to protect these devices
- Make sure you use a password that no-one else in the household knows or can guess
- Whilst working with school data, lock your screen whilst you are away/not using your device
- Check that all your devices fully up to date: anti-virus, malware and security updates
- Always be very careful which websites you visit and which email attachments you open
- Check that all local storage suitably encrypted? If you are unsure what this means ask at school
- Ensure that the devices cannot be stolen so please make sure they are always kept in a secure place. This applies to any hard copies (paper) of information that you take home too
- You must remove ALL data from your devices when it is no longer needed or at request from the school

DON'T

- Do not use USB data storage devices, they are so easy to lose or mis-place

 04.09.2023

REMEMBER

- Since the school is the data controller, you need to be aware that they may request to see the device to ensure the data is safe
- You must report ALL data breaches as instructed by your Data Protection lead and remember the time limits to which you must adhere – there is 72 hours in which to investigate and report a serious Breach to the ICO, play your part in ensuring this is achievable
- Remember your data protection training to help you to ensure that everything is kept safe whilst it's with you at home

Please follow normal school procedures to raise any concerns you have around protecting your school's personal data and if you need to report a Data Breach.