

Data Security – Do's and Don'ts for school staff

Passwords – Do

- use a strong password (see the National Cyber Security Centre advice)

Passwords – Don't

- share your passwords with anyone else or write them down
- save passwords in web browsers if offered to do so

Devices – Do

- try to prevent people seeing you enter passwords or view sensitive information
- log-off / lock your device when leaving it unattended

Devices – Don't

- use personal devices to view school-related or pupil data

Sending and sharing – Do

- be aware of who you are allowed to share information with. Check with your school data protection officer if you are not sure, who will check that third parties are GDPR-compliant
- only use encrypted removable media (such as encrypted USB pen drives) if ever taking any personal or sensitive data outside your school (which should be avoided and only done with permission)

Sending and sharing – Don't

- send sensitive information (even if encrypted) on removable media (USB drives, CDs, portable drives), if secure remote access is available.
- send sensitive information by email unless it is encrypted and use the systems that you are told to use

Accessing / saving data – Do

- only attempt to access data you are allowed to and save it on locations where your school knows that data is stored (the school must know where all data is and be able to access it)

Working on-site – Don't

- leave sensitive information unattended; lock it away in lockable drawers or log off or lock your work station
- let strangers or unauthorised people into staff areas
- position screens where they can be read from outside the room.

Working off-site – Do

- only take information offsite when you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above
- access data remotely instead of taking it off-site using approved secure systems
- make sure you sign out completely from any services you have used
- ensure you save to the appropriate directory to enable regular backups