**Data Protection Best Practice**

**Do:**

* Use “strong and long” passwords.
* Check consents whenever you are taking photos.
* Always lock your screen when away from it ( + L).
* Always take measures to de-personalise records, e.g. use initials not names.
* Only use first names (and surname initial if needed) where names are on display.
* On Birthday Charts, just show the month (not the full date).
* Secure sensitive information (e.g. safeguarding or medical information) when not in use.
* When posting, double-check postal addresses, and confirm with recipient and on your MIS.
* Dispose of personal data securely (shred or in confidential waste).
* Recognise that a request for personal data (e.g. from a parent, pupil or colleague) is a *Subject Access Request* and needs to be processed formally by your Data Protection Lead.
* Promptly report and concerns, breaches or incidents to your Data Protection Lead.

**When using email:**

* Be aware of malicious emails, and never open any unexpected links or attachments.
* Set up an email sending delay to give you a safety net to react to any errors.
* Use Blind Carbon Copy (BCC) when sending any email to more than one external recipient.
* When sending personal or sensitive data, get the recipient to email you first, and then reply to their email.

**Additionally, if you are working off-site, make sure you:**

* Only take the minimum personal data you need.
* Where possible, look to access or process personal data electronically (it’s more secure).
* Consider the protection of personal data when carrying out the school trip planning Risk Assessment.

**Don’t:**

* Use the same passwords across multiple sites or systems.
* ****Leave sensitive documents out on show where you are.
* Click on links or open attachments when sent by external email.
* Assume post is secure: always use Recorded or Special Delivery when sending sensitive information.
* Rely on local sources (e.g. planners or diaries) or email auto-fill for external contact information: always check your MIS.

**Additionally, if you are working off-site, make sure you don’t:**

* Take more personal data than you need.
* Take sensitive or special category data, unless it is absolutely essential.
* Download or save electronic files to personal devices.
* Leave your work email logged in on your personal device.