DATA PROTECTION EDUCATION

Your school is unique and data risks need to be assessed on an individual basis. For example:

- A school where the rooms are used for lettings has different risks to schools that are not.
- Larger schools with contract staff have different risks to smaller schools where all staff are directly employed.

GDPR and data protection is not about stopping you from doing your job, nor should it be thought of as something extra on top of your work. It's about making everyone think responsibly about data privacy and security every time you use data in your job.

Ask yourself... Would I be surprised if:

- You went into your GP surgery and your name, date of birth, gender, ethnicity and medical details were on display
- You had an appointment with your bank manager and all the bank's customer's details were displayed on the back wall - including yours

Would you be happy with this information being displayed without you being aware? Remember: Everyone is responsible for thinking about data protection and security of that data every time you use data in your job. **Including you**

USE THIS QUICK REFERENCE TO ENSURE YOU TREAT DATA WITH THE CONFIDENTIALITY AND INTEGRITY IT DESERVES

1 CUPBOARDS/ FILING CABINETS

ACTION POINTS	DETAILS TO BE AWARE OF
No storage	• Identify if existing storage can be re-arranged, prioritising the most confidential data. • Check other areas of the school for available storage. • Consider purchasing additional storage. • Avoid leaving sensitive files/data on open display.
Outdated information Sensitive files (i.e. educational psychology reports) Leaver information Folders (refer to Section 2)	• Get familiar with the information in your filing cabinets/cupboards. • Complete regular checks. • Securely destroy outdated information.
Unlocked cabinets	• Placing folders in cupboards/cabinets is better then leaving them out on open display. • If you have a key, lock at the end of each day, but make sure you have procedures and contingency to allow access in your absence.

2 FOLDERS (PHYSICAL)

How are folders stored? Are they kept on open display in the classroom? The type of folder that you may be in possession of could include, amongst others:
- Home school communication books
- Assessment/data folders
- Supply folders
- Behaviour folders
- Classroom files
- SEN folders

- Folders regularly contain outdated information. Check them regularly and securely destroy any data that is no longer needed.
- Where folders contain sensitive information, secure them away at the end of each day (end of day routines).
- If in doubt, check with your data lead.

3 FOLDERS (ELECTRONIC)

Do you know what is in your electronic folders?
When was the last time you completed a data cleanse?

Make sure you have an organised file structure to your data and then:
1. Check content
2. Delete outdated information

Ask yourself – if it's no longer needed why have you still got it?
If in doubt, check with your data lead.

4 LISTS AND DISPLAYS

Are class lists displayed with full name or forename only?
Avoid having the following on open display:
- Medical and allergy lists
- Video/photo consent 'No' lists
- Walk home alone lists
- Pupil Premium (PP) lists
- Lists with DOB and gender
- After school club lists

- Unless there is a teaching and learning justification try to use forename only.
- Lists that contain data such as: ethnicity, gender, SEN; pupil premium, date of birth, medical information etc could be located in folders. Make sure these are stored securely when unattended.
- Covering lists minimises unauthorised access but is not as secure as a folder system where the folder can be stored securely. Alternatively, identify if this information is available electronically and avoid physical copies.
- Displays: Consider the educational aim and whether you can achieve this aim with less, or no personal data at all. Use the minimum data possible.
- Do displays contain full name and where are the displays i.e. corridors. Who has access to the areas where displays are? Is your school used for lettings?
- Do your displays align with your schools consent form?

5 MEDICAL/SENSITIVE INFORMATION

ACTION POINTS	DETAILS TO BE AWARE OF
How is medical/health information stored and displayed in your school? Including: • Care plans • Medical/Allergy information • Student risk assessment data • Clinical/Educational Psychologists reports	• This is sensitive data and should be looked after with extra care. Don't leave reports/data/plans laying on desks, open trays, or drawers. Don't display on the walls of any unsecured locations. Ensure this information is filed correctly and secured. • When viewing sensitive data can it be read and viewed by anyone else in the room, or by people who enter the room? Use folder systems to make the information available, but not on display. • DPE understands this information is important. In fact we believe that it is so important a passive approach of displaying the information is inadequate. Rather we advocate using a secure system (physical or electronic) and take an active approach to informing relevant members of staff about this information.

6 LAPTOPS AND COMPUTERS

Laptops and computers left unattended and unlocked allow people to see sensitive data, either by accident or by design, accessing school systems when equipment is left alone and unrestricted.
Data observed from unlocked laptops:
Whole school data, including but not limited to:
- Staff CVs and personnel data
- Safeguarding data
- Performance management
- Progress/assessment data
- Contact information
- Medical information

Never leave your computer unattended. Ensure you lock it and at the end of each day switch off your equipment. Store your laptops and mobile devices securely.

- A quick way of locking your laptop/PC is to use the Windows + L key (⊞+ L).
- Try and close down your laptop/PC at the end of each day and store securely away.
- Can monitors be viewed by parents, or people external to the school? If so readjust screens, or consider a privacy screen.
- Only computers and devices that can be encrypted should be removed from the school.

7 PHOTOS

Digital media and photos:

- Do you have old photos on cameras, laptops, tablets and network?
- Do you have routines for removing photos from portable devices?
- Are there old cameras laying around? What data is stored on SD cards?

- Regularly check your electronic folders and delete data no longer needed.
- Add 'whole school' photos/videos that are being kept for archiving and historical purposes to your archived folder. If you're not sure how to do this, contact your IT department, or get your data lead to contact DPE for advice.

Photo with full name	• Check your schools consent guidelines. • Photos with full name should generally be avoided for displays. Always ask yourself if you can manage with less data.

8 CONFIDENTIAL WASTE

Be careful with how you dispose of and store confidential waste. For example:
- Staff salary and financial details left in offices (waiting to be shredded)
- Student assessment details in waste bins
- Confidential waste sacks left open and not secured

- If data is confidential don't rely on someone else to dispose of the data, take responsibility to destroy it yourself immediately.
- If it is stored prior to external destruction make sure it is securely stored into secure bins.
- Avoid leaving in open sacks or boxes. Confidential waste bags and boxes must be kept as securely as befits the documents they hold.

9 PRINTING/PHOTOCOPYING

ACTION POINTS	DETAILS TO BE AWARE OF
Be aware of issues including: • Confidential data getting mixed with class resources • No option to select confidential printing • No codes at printer/photocopier • Printing left unattended on printers and photocopiers	• Add confidential printing codes. • If you need to print confidential material, ensure you select a printer that is secure. • If you send something to print, collect it, don't forget it.

10 MEMORY STICKS/PORTABLE HARD DRIVES

School data stored on memory sticks/portable hard drives:
Do you still use an unencrypted memory stick?
Do you use your own portable storage?

Portable storage (USB, hard-drives, memory cards) should be avoided. Even if encrypted, they are easily lost or data corrupted and can easily transfer malware and viruses from infected computers.
Cloud-based storage, or remote network login is safer and more secure.
If you have no choice than using portable storage, it must:
- Be encrypted.
- Not used for long-term storage.
- Only used for the files you are currently working on, which when completed, transferred back onto the main school network/storage, and files securely deleted.
- Virus and malware checked prior to use of any files.

11 EMAILS

Using, sending and storing emails

- Encrypt emails that contain private and confidential data.
- Never send passwords to encrypted emails or files through the same email system - use alternatives e.g. SMS text?
- Use secure systems (i.e. ParentMail/Schoolcomms) for sending information to parents.
- Write your email and subject line first - add in the recipients last.
- If using BCC, be careful that you don't accidentally use CC and use a second pair of eyes to check prior to sending.
- Tidy and declutter your inbox - delete emails you no longer need.
- Do not use email for long-term storage -move important data into an appropriate file.
- Save any email text/attachment which needs to be retained in an appropriate system/file.
- Don't put personal information in the subject line.
- Avoid adding email addresses manually and try not to use 'autofill' for retrieving email addresses without double checking.

12 AFTER SCHOOL

Site security – are doors wedged open and school gates left open after school? Who can enter the school when most of the staff have gone home? Are internal doors, cupboards and cabinets locked at night?

If it was your data, would you give anyone open access to your information?
Treat other people's data as if it were your own.

- Check how open/secure your school is when pupils have gone home.
- Develop end of day routines to ensure all your data and devices are secured at night.
- Operate a clear desk policy.
- Ensure doors and windows are locked at night.

THINK who else has access when you've left the school, For example:
Is your school used by extended services?
Do you let parts of the schools to clubs and societies?
Do you have contract cleaners
Do contract staff regularly visit the school
What could someone access from your unlocked laptop/PC?