



DATA PROTECTION QUICK GUIDE

For Emergency & Supply Teaching Staff

A companion resource in the Data Protection for Operational Staff series

This guidance is for staff covering lessons at short notice, including emergency and day-to-day supply cover. It applies whether or not you've had time to complete the school's full induction, and compliance with UK GDPR, safeguarding requirements, and school policy is mandatory regardless of how much notice you were given.

Who to Contact Today

Ask the school office to complete this before you start, if it isn't already filled in:

Role	Name	Contact / Location
Designated Safeguarding Lead (DSL)	...	...
School Office	...	...
Data Protection Champion	...	...
IT Support (for cyber issues)	...	...

[SCHOOL TO INSERT: link to safeguarding policy on the school's own website]

Key Principles

- Do not access any school system containing personal data (SIMS, Arbor, CPOMS, email, etc.) unless you have completed the school's mandatory Cyber Security and Data Protection training, or been given a verbal briefing and supply login details.
- Only use printed registers and materials provided by the school office for attendance and safeguarding purposes.
- Do not remove any personal data from the school premises under any circumstances. This includes photos, notes, or anything taken home to mark.
- Return all printed registers and documents to the school office before you leave, every day.
- Keep personal data confidential at all times. Do not discuss pupil information outside the classroom or with anyone not authorised to hear it.

Disclaimer: These resources are for general educational purposes only and are provided "as is." While we strive for accuracy, Data Protection Education makes no warranties regarding completeness or suitability. Use of these materials does not constitute professional legal or data protection advice; please seek independent counsel for your specific circumstances. To the extent permitted by law, we are not liable for any losses arising from the use of these resources. All intellectual property remains with Data Protection Education; personal or internal organisational use is permitted subject to our terms and conditions.



- Follow the school's own safeguarding procedures for handling pupil information. Ask the school office for the safeguarding policy and the name of the Designated Safeguarding Lead (DSL) on arrival.

If Something Goes Wrong: Contain, Secure, Report

If you discover unsecured personal data, lose a register, send information to the wrong person, or anything else feels like a data protection risk, follow the same three steps used across the school:

1. **Contain:** Stop the risk from spreading. Don't photograph, forward, or discuss it further while you work out what's happened.
2. **Secure:** Move papers into a locked room, cover them, or otherwise put them out of view immediately.
3. **Report:** Tell the school office or Data Protection Champion straight away, even if you've already fixed it. Speed matters: schools may have only a limited window to report certain incidents onward.

This applies to emergency situations too, for example:

- Evacuating during a fire alarm or lockdown while holding a register: bring it with you if safe to do so, but do not leave it unattended once the situation is over.
- A pupil discloses a safeguarding concern to you during a lesson: do not investigate or promise confidentiality. Note only what was said, when, and by whom, and report it to the DSL immediately.
- You realise partway through the day that you've already left a register or device unsecured: report it as soon as you notice, rather than waiting until the end of the day.

If You Haven't Had Full Induction

Same-day emergency cover doesn't always allow time for the school's full mandatory training before you start teaching. Where that's the case, the school office or your point of contact should give you a short verbal briefing covering:

- Who the DSL is and how to reach them today
- Where printed registers are kept and returned
- Who the Data Protection Champion or IT contact is for this site

You should still avoid logging into any school system until you have completed the full training. The briefing covers what to do in the meantime, not a substitute for it.

Disclaimer: These resources are for general educational purposes only and are provided "as is." While we strive for accuracy, Data Protection Education makes no warranties regarding completeness or suitability. Use of these materials does not constitute professional legal or data protection advice; please seek independent counsel for your specific circumstances. To the extent permitted by law, we are not liable for any losses arising from the use of these resources. All intellectual property remains with Data Protection Education; personal or internal organisational use is permitted subject to our terms and conditions.



Do and Don't

DO	DON'T
Keep printed registers secure and out of sight when not in use.	Take photos of registers or share data electronically.
Return all printed materials to the office before you leave.	Leave printed registers unattended, even briefly.
Ask the school office for a short briefing if you've arrived at short notice.	Attempt to log in to any school system without completed training.
Report suspicious emails, calls, or activity immediately.	Share personal data with anyone outside the school.

Quick Cyber Security Tips

- Never click links or open attachments in unexpected emails. A common warning sign is urgency, e.g. being told to act immediately or enter a password.
- Lock your device whenever you step away from it, even for a moment.
- If you're given temporary login access, only use it if authorised, and use a strong, unique password.
- Be alert to "vishing": phone calls pressuring you to reset a password or share sensitive information. Hang up and report it rather than complying.

Acknowledgement

I confirm I have read and understood this guidance.

Name: _____ Date: _____

Signature: _____

Disclaimer: These resources are for general educational purposes only and are provided "as is." While we strive for accuracy, Data Protection Education makes no warranties regarding completeness or suitability. Use of these materials does not constitute professional legal or data protection advice; please seek independent counsel for your specific circumstances. To the extent permitted by law, we are not liable for any losses arising from the use of these resources. All intellectual property remains with Data Protection Education; personal or internal organisational use is permitted subject to our terms and conditions.