Data Handling Security Policy

Changes since last edition:

- *Added Governors to introductory paragraph*
- *Additional point 20 added to state new technology must not be used before completion of a DPIA*
- *Additional point 21 added to state you must add delegates to your emails*

You are the custodian of the equipment and data issued to you to carry out your role; it is your responsibility to keep it physically secure.

This policy sets out the rules all staff, governors, contractors and volunteers **must** follow when managing IT equipment, removable storage devices and papers, in the office, in transit and at home or other work locations.

Policy rules:

1. You must take **responsibility** for the security of the equipment allocated to you and that is in your custody.
2. When you are physically **transporting** our data outside of our premises, on any medium, you must take steps to keep it secure
3. You must not leave Official-Sensitive data unattended in a **vehicle** for longer than 10 minutes, and always keep it out of sight
4. You must take appropriate steps to secure our data when working at **home** or other organisations' **premises**
5. If working with our data on approved unmanaged equipment (personal devices), you must **remove** the data when finished, including from cloud storage, and prior to leaving the school's employment
6. If you are taking Official-Sensitive information out of the school, this must be **recorded**
7. You must make sure that conversations discussing sensitive data are only audible by an **appropriate audience**
8. You must not allow anyone to **access** to your IT equipment through your IT account

9. You must not store our business data on any equipment, including personal devices, which has not been **approved**
10. You must not allow unauthorised people to be able view information on your IT equipment **display**
11. You must not save your **passwords** to any web-based system which holds our data in the browser
12. You must always use an approved secure method of **disposing** of physical documents and data storage devices
13. You must **return** all equipment which has been issued to you by us, prior to leaving your employment
14. You must **report** as quickly as possible if your equipment is lost or stolen and assist with any **investigation**
15. You must ensure that all security functions are **enabled** on your portable equipment, such as pin codes and password access
16. You must keep your portable equipment, **clean and serviceable**, including keeping it charged
17. You must not take any of our equipment **abroad** unless you are traveling in a business capacity with approval
18. You must not give your portable equipment to **another person** if you are not using it.
19. You must immediately raise as a **data breach** any loss, unlawful access or theft of the data we are responsible for
20. You must not use new technology that collects personal data (e.g. learning platforms, apps etc) before it has been assessed by completion of a Data Protection Impact Assessment (**DPIA**)
21. You must add **delegates** to your email account, so that your business emails can always be accessed when you are on leave. Two delegates are recommended, one of which should be your manager.

How must I comply with these policy rules?

We have related policies, procedures and guidance which help you comply with these rules. These include:

- Data Protection Policy
- Data Breach Policy
- Records Management Policy
- Data Breach Procedure

If you are unsure how to comply you must seek advice and guidance from your Data Protection Lead.

What if I need to do something against this policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school office.

Reference

- Data Protection Act 2018 / UK GDPR
- Article 8, The Human Rights Act 1998

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Document Control

Version:	2025
Date approved:	10th July 2025
Approved by:	FGB
Next review:	Annual

