Acceptable Personal Use of Resources and Assets Policy

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. It is reasonable to assume that at times, staff may use our IT and other facilities resources for personal reasons. However, it is important that boundaries are set to ensure that this is done effectively so that our reputation is maintained and staff working time is used efficiently on delivering our business outcomes.

This policy sets out the rules all staff, governors, contractors and volunteers must follow when using resources and assets provided by the school, including IT facilities, for personal use. It aims to ensure that everyone understands their professional responsibilities when using any form of ICT.

Policy rules:

1. You must use our facilities **economically**; your personal use must not create extra costs for us
2. You must not use our facilities to undertake any unlawful, libellous, immoral or offensive **activities**, including accessing, downloading, storing, creating, copying or disseminating offensive material. This includes, but is not limited to, pornographic, sexual, violent or criminal content and racist, sexist or otherwise discriminatory material
3. Personal use must not interfere with your **productivity** and how you carry out your duties
4. Personal use must not reflect adversely on our **reputation**
5. You must not leave **personal-use websites** open during your working time, even if they are minimised on your screen and you are not actively viewing/ using them
6. You must not use browsers or access/ attempt to access sites that are knowingly **unacceptable**, even if this is in your own time
7. You must not **send or forward** chain, joke or spam emails
8. You must not use the Organisation's facilities for **commercial purposes** not approved by us or for personal financial gain
9. You must not use your access rights or identity as an employee to **mislead** another person, for personal gain or in any other way which is inconsistent with your role
10. You must not **disclose** (in writing, speech or electronically) information held by us unless you are authorised to do so, and the recipients are authorised to receive it
11. When you print, photocopy or scan official-sensitive information, you must not leave the information **unattended**
12. You must not **connect** any equipment to our IT network that has not been approved

13. You must not do anything that would **compromise** the security of the information held by us. This includes downloading or opening files from an unknown or untrusted source as these may introduce a virus or malware; or disabling or changing standard security settings.
14. You must not make personal use of the information available to you that is not available to the **public**

How must I comply with these policy rules?

By complying with the policy rules set out above and checking with your manager when you have any uncertainty over what is appropriate. We have related policies, procedures and guidance which will help you how to comply with these rules. These include:

- Data Handling Security Policy
- Data Breach Policy
- Records Management Policy
- Data Breach Procedure
- Retention Schedule

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 Data Protection Lead.

References

- Data Protection Act 2018 / UK GDPR
- Computer Misuse Act 1990
- Data Use & Access Act 2025

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:	2026
Date approved:	May 2026
Approved by:	CEO – Mr C Jones
Next review:	May 2027

