Robert Clack School of Science

Computer Resources, Cyber Security and Acceptable Use Policy 2026 - 2027

Approved by Executive Headteacher: **Date:** September 2026

Signed by Chair of Governors: **Date:** September 2026

Last reviewed on: September 2026

Next review due by: September 2029

Contents

1. Purpose 3
2. Scope 3
3. General User Responsibilities 3
4. IT Equipment 3
5. Personal Use 3
6. User Accounts 3
7. Passwords and Multi-Factor Authentication 3
8. Data Protection 3
9. Handling Sensitive Information 3
10. Cloud-First Storage 4
11. USB Storage and Removable Media 4
12. Cyber Security Responsibilities 4
13. Incident Reporting and Response 4
14. Email and Communications 4
15. Internet and Social Media Use 4
16. School Wireless Services 4
17. Mobile Devices 4
18. Remote Working and Online Meetings 4
19. Safeguarding 5
20. Monitoring and Compliance 5
21. Loaned Equipment 5
22. Staff Leaving the School 5
23. Policy Breaches 5
Appendix A – Cyber Security Quick Reference 6

1. Purpose

Robert Clack School provides access to digital systems, cloud services and information resources to support teaching, learning and administration. This policy establishes the standards expected for the safe, secure and professional use of those resources.

2. Scope

Applies to employees, agency staff, contractors, consultants, students, parent-carers with authorised access and visitors using school technology resources. Applies to Microsoft 365, Teams, SharePoint, OneDrive, RM Unify, Google Workspace, Bromcom MIS, Arbor Finance, school wireless services and personal devices accessing school systems.

3. General User Responsibilities

Cyber security, safeguarding and data protection are the responsibility of all users. Users must protect school information, comply with school policies, respect others and report concerns immediately.

4. IT Equipment

School equipment must be used for authorised purposes only. Software installations, equipment moves and configuration changes require authorisation. Faults must be reported through approved ICT support procedures.

5. Personal Use

Limited personal use is permitted where it is lawful, appropriate, does not interfere with professional responsibilities and complies with school policies.

6. User Accounts

Accounts remain the responsibility of the account holder. Credentials must never be shared. Generic accounts require formal approval. Suspected compromise must be reported immediately.

7. Passwords and Multi-Factor Authentication

Users must maintain strong passwords or passphrases in accordance with NCSC guidance. Passwords must be changed immediately if compromise is suspected or when instructed by ICT Services. Multi-Factor Authentication (MFA) is mandatory for Microsoft 365, RM Unify, Google Workspace, Bromcom MIS, Arbor Finance and other designated systems. Users must never share passwords, MFA codes or approve unexpected MFA prompts.

8. Data Protection

All users must comply with UK GDPR and Data Protection legislation. Confidential information must only be accessed where authorised and must be protected from unauthorised disclosure.

9. Handling Sensitive Information

Sensitive information must be handled securely at all times. Users must verify recipients before sharing information and protect information when working remotely.

10. Cloud-First Storage

Robert Clack School adopts a cloud-first approach. Approved storage locations include Microsoft OneDrive, SharePoint, Teams, Google Drive and Google Classroom. Approved cloud services should be used in preference to removable media.

11. USB Storage and Removable Media

Removable media should only be used where a legitimate business requirement exists and written approval has been granted. Annual exemption reviews apply. Lost or stolen removable media must be reported immediately.

12. Cyber Security Responsibilities

Cyber security is the responsibility of all users. Users must remain vigilant against phishing, social engineering, malware and online scams, keep devices secure and report suspicious activity immediately.

13. Incident Reporting and Response

All users must immediately report phishing attacks, malware infections, account compromise, data breaches, lost devices, lost removable media, safeguarding concerns and unauthorised access attempts. Users who report genuine mistakes promptly will be supported. Attempts to conceal incidents may be treated as a disciplinary matter.

14. Email and Communications

School email must be used for official school business. Email forwarding to personal accounts is prohibited. Suspicious messages must be reported immediately.

15. Internet and Social Media Use

Users must not access services intended to bypass school filtering or safeguarding controls. Internet use must be lawful, professional and appropriate.

16. School Wireless Services

Wireless usage is subject to monitoring and filtering. Guest access is provided only through approved school procedures.

17. Mobile Devices

Devices accessing school systems must be secured using a PIN, password or biometric authentication. Lost, stolen or compromised devices must be reported immediately.

18. Remote Working and Online Meetings

Professional standards apply when working remotely. School systems should not be accessed via unsecured public Wi-Fi unless protected through an approved secure connection method.

19. Safeguarding

Online safeguarding concerns, harmful content and illegal material must be reported immediately through safeguarding procedures. Evidence should be preserved and not investigated by users.

20. Monitoring and Compliance

The school may monitor networks, systems, internet services, cloud services and email systems for safeguarding, operational, legal, regulatory and cyber security purposes.

21. Loaned Equipment

Loaned equipment remains school property and must be used in accordance with school policies and loan agreements.

22. Staff Leaving the School

Staff must complete handovers, transfer resources and return equipment before leaving. A discretionary cloud-access grace period of up to 60 days may be approved where there is a legitimate operational requirement.

23. Policy Breaches

Breaches may result in withdrawal of access, management action, disciplinary procedures or referral to external authorities where appropriate.

Appendix A – Cyber Security Quick Reference

- Use MFA on all supported systems
- Never share passwords or authentication codes
- Report suspicious emails immediately
- Report lost devices immediately
- Report data breaches immediately
- Store files in approved cloud services
- Avoid public Wi-Fi for school access
- Keep devices secure and updated
- Report incidents promptly
- When in doubt, report it