



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. Introduction	3
2. School IT Equipment	5
3. Security of School Data	8
4. Cyber Safety and Vigilance	12
5. School Wireless Network.....	13
6. Account Security and Authentication.....	14
7. USB Storage, Cloud Storage (OneDrive and Google Drive).....	17
8. Internet – Internet Filtering	18
9. Handling Sensitive Information	19
10. Cloud-First Storage.....	21
11. Personal Activities	23
12. Remote Learning, Online Meetings and Digital Collaboration	24
13. Social Networking	27
14. Safeguarding Issues	28
15. Working Away From School	29
16. School Loaned Computer Equipment.....	30
17. Leaving Robert Clack School	31
18. Closing Statement	34

1. Introduction

This Acceptable Use Policy ("AUP") sets out the conditions under which users may access and use Robert Clack School's Information Technology (IT) systems, services, networks, devices and digital resources.

The policy applies to all access to school systems, whether:

- On school premises or off-site.
- Through school-owned or personal devices.
- Using wired, wireless or remote connections.
- Accessing data stored locally or within cloud-based services.

This policy applies to all information systems and digital services provided, managed, licensed or authorised by Robert Clack School, including but not limited to:

- Microsoft 365 (including Outlook, OneDrive, SharePoint and Teams, together with any future Microsoft services and applications licensed by the School)
- Google Workspace for Education
- RM Unify
- Bromcom MIS
- CPOMS
- Arbor Finance
- School websites and online platforms
- School managed networks and wireless services

Compliance with this policy is mandatory and forms part of the school's wider responsibilities relating to:

- Safeguarding
- Information Security
- Data Protection (UK GDPR and Data Protection Act 2018)
- Professional Conduct
- Cyber Security

Access to school systems is provided for educational and professional purposes and is granted as a privilege, not a right. The school reserves the right to suspend or remove access where misuse is identified.

Failure to comply with this policy may result in:

- Removal of access privileges
- Internal disciplinary action
- Referral to external agencies
- Criminal or civil proceedings where appropriate

1.1 Definitions

For the purposes of this policy:

School

"School", "Robert Clack School" or "Robert Clack School of Science" refers to all facilities, networks, systems, services and digital resources operated by or on behalf of Robert Clack School, including Robert Clack Primary School and the Robert Clack Leisure Centre where applicable.

Network

"Network" refers to all school-managed technology infrastructure including:

- Internal wired and wireless networks
- Internet connectivity
- School servers and storage systems
- Cloud services
- School domains and associated authentication services

User

A "User" means any person authorised to access school systems, including:

- Employees
- Agency staff
- Contractors
- Governors
- Volunteers
- Students
- Parent-Carers with authorised access
- Third-party support providers

School Data

"School Data" means any information created, stored, processed or transmitted on behalf of the school, including:

- Pupil information
- Staff information
- Safeguarding records
- Financial information
- Assessment data
- Curriculum resources
- Email correspondence
- Documents stored in cloud platforms

1.2 General Principles

All users must:

- Use school systems safely, responsibly and professionally.
- Protect the confidentiality, integrity and availability of school data.
- Comply with the requirements of UK GDPR and the Data Protection Act 2018.
- Follow all safeguarding requirements.
- Take reasonable steps to protect school systems from cyber threats.
- Report any suspected security incident, data breach or safeguarding concern immediately.

Users must not:

- Attempt to gain unauthorised access to systems or data.
- Share accounts or passwords.
- Use systems in a manner that could damage the school's reputation.
- Engage in unlawful, offensive, abusive or inappropriate activity.
- Circumvent security controls implemented by the school.

2. School IT Equipment

Robert Clack School provides Information Technology equipment, software, digital resources and related services to support teaching, learning, administration and the day-to-day operation of the School. All users are expected to use School equipment responsibly, safely and in accordance with this policy.

2.1 Use of School Equipment

School-owned devices, systems and digital resources must be used primarily for authorised educational, professional and administrative purposes.

Users must take reasonable care of all School-owned equipment and ensure that it is used in accordance with any instructions, guidance or training provided.

Examples of School IT equipment include, but are not limited to:

- Desktop computers
- Laptops and tablets
- Interactive displays and projectors
- Printers and multifunction devices
- Mobile devices
- Network and wireless equipment
- Audio-visual equipment
- Peripheral devices such as keyboards, mice, webcams and headsets

2.2 Care and Protection of Equipment

Users must:

- Take reasonable precautions to prevent loss, theft or damage.
- Report any faults, damage, loss or suspected theft immediately through the School's designated support procedures.
- Ensure equipment is stored securely when not in use.
- Follow all health and safety guidance relating to the use of IT equipment.

Users must not:

- Deliberately damage, interfere with or misuse School equipment.
- Deface equipment or remove School asset labels, identification tags or security markings without authorisation.
- Use equipment in a manner likely to cause damage to the device, network or other School systems.

Deliberate damage, theft or misuse of School equipment may result in disciplinary action and, where appropriate, recovery of costs.

2.3 Movement and Relocation of Equipment

School equipment must not be moved, relocated, loaned or transferred to another room, department or site without appropriate authorisation.

This requirement applies to both fixed and portable equipment, including monitors, printers, laptops, docking stations and peripheral devices.

Any permanent relocation of equipment must be coordinated through the Technical Support Team to ensure that asset records remain accurate.

2.4 Installation of Software and Applications

Only software, applications, browser extensions and digital tools that have been approved by the School may be installed on School-owned devices.

Users must not:

- Download or install unauthorised software.
- Attempt to bypass software restrictions.
- Install software that may present a cybersecurity, safeguarding, licensing or data protection risk.

Requests for additional software should be submitted to the Technical Support Team for review and approval.

The School reserves the right to remove any unauthorised software or application from its systems.

2.5 Connection of Devices and Accessories

Only authorised devices may be connected to School systems and networks.

Users must not connect personal devices, storage media, network equipment or accessories to School systems unless permission has been granted and any required security checks have been completed.

The School reserves the right to restrict or block devices that present a security, safeguarding or operational risk.

2.6 Printers and Technical Maintenance

The maintenance, repair and configuration of School IT equipment is the responsibility of authorised personnel.

Users must not attempt repairs or modifications to School equipment unless specifically authorised to do so.

Where equipment develops a fault, users should report the issue through the School's designated IT Helpdesk or support process.

2.7 Food and Drink

Food and drink should be kept away from School IT equipment wherever practical.

Users may be held responsible for damage resulting from negligence, carelessness or failure to follow reasonable precautions.

2.8 School-Issued Devices

Staff or students who are issued with School laptops, tablets or other mobile devices remain responsible for those devices while they are in their possession.

School-issued devices:

- Remain the property of Robert Clack School.
- Must be returned upon request or when employment, enrolment or the loan agreement ends.
- May be subject to monitoring, management and security controls.
- Must be used in accordance with this Acceptable Use Policy and all related School policies.

Users must immediately report the loss, theft or compromise of any School-issued device.

2.9 Monitoring and Security Controls

School IT equipment may contain monitoring, safeguarding, endpoint protection, device management and security software designed to protect users, systems and data.

Users must not:

- Attempt to disable, remove or interfere with security controls.
- Circumvent monitoring or safeguarding systems.
- Use tools designed to evade School security measures.

Any suspected attempt to bypass School security controls may be investigated and may result in disciplinary action.

3. Security of School Data

Robert Clack School processes and stores information relating to students, staff, parent-carers, governors, contractors and other individuals in the course of its educational and operational activities.

All users have a responsibility to ensure that School Data is protected against unauthorised access, loss, theft, alteration, disclosure or destruction. The handling of School Data must comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and all relevant School policies and procedures.

3.1 Access to School Data

Users must only access information that is necessary for the performance of their role and for legitimate School purposes.

Users must:

- Access only information they are authorised to view.
- Respect the confidentiality of personal, safeguarding, financial and operational information.
- Ensure information is only shared with authorised individuals who have a legitimate need to know.
- Follow the principle of least privilege when accessing systems and information.

Users must not:

- Access records for personal interest or curiosity.
- Access information relating to family members, friends, colleagues or students unless required by their professional duties.
- Share confidential information with unauthorised persons.

Unauthorised access to School Data may result in disciplinary action and may constitute a breach of data protection legislation.

3.2 Protection of School Data

The security of School Data is the responsibility of every user entrusted with access to that information.

Users must:

- Store School Data only on approved School systems and platforms.
- Follow School security procedures when handling confidential information.
- Ensure devices used to access School Data are appropriately secured.
- Lock or sign out of devices when unattended.
- Report suspected security incidents immediately.

Approved storage locations include:

- Microsoft OneDrive
- Microsoft SharePoint
- Microsoft Teams
- Google Drive
- Bromcom
- CPOMS
- Arbor Finance
- Other School-approved systems

School Data must not be stored on unauthorised third-party services, personal cloud storage platforms or personal email accounts.

3.3 Account Security

Access to School systems is granted through individual user accounts and secure authentication methods.

Users must:

- Keep passwords and authentication methods confidential.
- Use Multi-Factor Authentication (MFA) where required.
- Immediately change passwords if compromise is suspected.
- Report any suspected compromise of an account to their Line Manager and the Technical Support Team.

Users must not:

- Share usernames, passwords or authentication devices.
- Permit another person to access School systems using their account.
- Attempt to access systems using another user's credentials.

The forwarding of School email to external email addresses, including personal email accounts, is prohibited.

3.4 Transfer and Storage of Data

Confidential, personal and sensitive School Data must be handled securely at all times.

Users must not:

- Copy School Data to personal devices without authorisation.
- Transfer School Data to unauthorised systems or services.
- Store confidential information on removable media unless expressly authorised.
- Transfer School Data using insecure methods.

Where there is a legitimate operational requirement to transfer data:

- Approved School systems should be used wherever possible.
 - Appropriate encryption and security controls must be applied.
-

- The transfer must comply with School Data Protection procedures.

The use of USB devices and other removable media remains subject to the School's USB Storage Policy.

3.5 Display and Use of Confidential Information

Users must take reasonable steps to prevent confidential information from being disclosed to unauthorised persons.

Particular care should be taken when:

- Using classroom displays and projectors.
- Conducting staff meetings.
- Working in shared environments.
- Delivering remote lessons or meetings.
- Accessing information from home or other remote locations.

Except where specifically required for teaching, learning or administrative purposes, confidential information should not be displayed on screens visible to unauthorised individuals.

Confidential information held within Bromcom, CPOMS or other School management systems must only be accessed and displayed where there is a legitimate educational or operational need.

3.6 Printing and Disposal of Confidential Information

Printing confidential or sensitive information should be kept to a minimum and only undertaken where there is a legitimate business requirement.

Any printed confidential material must:

- Be collected promptly from printers.
- Be stored securely.
- Not be left unattended.
- Be disposed of using approved confidential waste or shredding procedures.

Users should consider whether electronic storage and sharing methods provide a more secure alternative before printing information.

3.7 Images, Photography and Digital Media

Personal cameras, smartphones or other personal devices must not be used to capture, store or transfer images, videos or recordings of students or staff unless expressly authorised and undertaken in accordance with School policies.

Any images, recordings or digital media created as part of School activities must:

- Be stored securely.
- Be retained only for as long as necessary.
- Be processed in accordance with safeguarding and data protection requirements.

3.8 Data Breaches and Security Incidents

Users must immediately report:

- Suspected data breaches.
- Loss or theft of a device containing School Data.
- Unauthorised disclosure of information.
- Misdirected emails containing personal data.
- Suspected account compromise.
- Any other incident that may affect the confidentiality, integrity or availability of School Data.

Reports should be made immediately through the School's designated incident reporting process or Helpdesk system and escalated as appropriate to:

- The Technical Support Team
- The Data Protection Officer (where applicable)
- A Line Manager
- The Senior Leadership Team where appropriate

Prompt reporting allows the School to meet its legal obligations and minimise potential harm.

4. Cyber Safety and Vigilance

Technology plays a critical role in the operation of the School and the education of students. To ensure that these systems remain secure, reliable and available, they must be protected against cyber threats, data breaches and other forms of malicious activity.

Cyber security is a shared responsibility. The School and all users of its systems are expected to exercise appropriate vigilance and take reasonable steps to protect School devices, accounts, systems and information assets. Where there is clear evidence of negligence or a failure to exercise due diligence, disciplinary action may be considered.

Any device used to access School systems, whether School-owned or personal, must be appropriately secured and maintained. Users who have concerns regarding the security of a device used for School business should seek advice immediately from the Technical Support Team.

Compliance with this Acceptable Use Policy forms part of each user's responsibility to maintain a secure working environment and to safeguard School information and resources.

The key principles of cyber safety are:

- Maintaining vigilance when handling emails and other electronic communications.
- Never sharing login credentials, passwords, authentication codes or security tokens with any other person.
- Never leaving passwords or authentication information visible to others.
- Maintaining strong passwords and changing them immediately if compromise is suspected.

- Ensuring that Multi-Factor Authentication (MFA) is enabled and maintained where required.
- Taking reasonable steps to ensure that personal devices used to access School systems are appropriately protected, updated and free from malicious software.
- Avoiding access to School systems through public or unsecured Wi-Fi networks unless appropriate security measures are in place.
- Familiarising themselves with current cyber security guidance provided by the National Cyber Security Centre (NCSC).

Users are encouraged to regularly review the latest cyber security advice available from the NCSC:

<https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools>

Failure to follow these principles may expose the School to cybersecurity risks, data breaches, financial loss and reputational damage and may result in disciplinary action where appropriate.

5. School Wireless Network

Staff users may access the School Wireless Network where this service is available. By connecting to the School Wireless Network, users agree to comply with this Acceptable Use Policy regardless of whether the connecting device is School-owned or personally owned.

Access to the School Wireless Network is provided using individual School user credentials. Users are responsible for all activity conducted through their accounts and must take reasonable steps to protect their login details from unauthorised use.

Users should be aware that any device connected to the Robert Clack School Wireless Network is subject to the School's internet filtering, monitoring and safeguarding systems in accordance with School policies, safeguarding obligations and applicable legislation.

Under no circumstances should users disclose their School username, password or authentication credentials to another person. Providing login credentials to students or any unauthorised individual will be regarded as a serious breach of School Policy and may result in disciplinary action and the removal of access privileges.

Students are not permitted to access the School Wireless Network, except for Sixth Form students who are authorised to access designated wireless services using their own School-issued user credentials and in accordance with School policy.

The School provides a guest wireless service for authorised visitors who have registered through the School's visitor management system. Guest wireless credentials are managed by the School and are changed periodically to maintain security. Guest access credentials must not be shared with students unless the student is under the direct supervision of an authorised member of staff and access has been approved for a legitimate educational purpose.

Users connecting personal devices to the School Wireless Network remain responsible for ensuring that those devices are adequately secured, updated and protected against malware and other cyber threats.

Failure to comply with the requirements of this section may result in the withdrawal of wireless access privileges and, where appropriate, disciplinary action.

6. Account Security and Authentication

Robert Clack School uses account authentication controls to protect users, devices, systems and School Data from unauthorised access.

All users are responsible for maintaining the security of their accounts and authentication credentials. Failure to do so may place School systems, confidential information and individuals at risk.

6.1 User Accounts

Each user will be provided with one or more individual accounts to access School systems and services.

Accounts are issued on a named-user basis and must only be used by the individual to whom they have been assigned.

Users must:

- Use only their own authorised account(s).
- Ensure that account credentials remain confidential.
- Log out of systems or lock devices when unattended.
- Notify the Technical Support Team immediately if account compromise is suspected.

Users must not:

- Share usernames or passwords.
- Allow another person to use their account.
- Use another person's account without authorisation.
- Circumvent authentication or security controls.

Access to School systems may be suspended where misuse, compromise or unauthorised access is suspected.

6.2 Federated Services and Single Sign-On (SSO)

The School operates federated authentication services to provide secure access to multiple systems using a single set of credentials.

These services currently include, but are not limited to:

- RM Unify
- Microsoft 365
- Google Workspace for Education
- Active Directory and associated School systems

Where services are federated, a password change made through the designated authentication system will automatically update linked services.

Users should be aware that changes may take a short period of time to synchronise across all connected platforms.

6.3 Password Requirements

All users must create and maintain strong passwords in accordance with current School security requirements.

Passwords should:

- Be difficult for others to guess.
- Be unique to the user.
- Not be based on easily obtainable personal information.
- Not be reused across personal and School systems.

Users must not:

- Share passwords with any other person.
- Write passwords where they can be accessed by others.
- Store passwords insecurely.
- Use another person's credentials.

Where there is evidence or suspicion that a password has been compromised, it must be changed immediately.

The School may require password changes where security risks are identified.

6.4 Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA), also known as Two-Factor Authentication (2FA), provides an additional layer of security beyond a username and password.

MFA is mandatory for all staff access to designated School systems, including:

- Microsoft 365
- Google Workspace
- RM Unify
- Bromcom
- Arbor Finance
- Any other systems designated by the School

Users must:

- Maintain access to their registered authentication method.
 - Promptly report any loss or replacement of an authentication device.
 - Follow School guidance regarding MFA registration and management.
-

Users must not:

- Approve authentication requests that they did not initiate.
- Share authentication devices or verification codes with others.

Any unexpected MFA prompt should be treated as a potential security incident and reported immediately.

6.5 Account Compromise

A user who believes that their account may have been compromised must take immediate action.

Examples include:

- Accidental disclosure of credentials.
- Unexpected MFA prompts.
- Suspicious login notifications.
- Unauthorised password changes.
- Evidence of unauthorised activity within an account.

Users must immediately:

1. Change their password where possible.
2. Notify the Technical Support Team.
3. Inform their Line Manager where appropriate.
4. Follow any additional security instructions provided by the School.

Prompt action may prevent wider compromise of School systems and data.

6.6 Shared and Generic Accounts

Individual named accounts must be used wherever possible.

Shared, departmental or generic accounts will only be permitted where:

- There is a legitimate operational requirement.
- Approval has been granted by the Senior Leadership Team.
- Appropriate auditing and security controls are in place.

Any shared account must have a clearly identified owner responsible for its use and security.

6.7 Leavers and Account Removal

Access to School systems will be removed when a user no longer requires access due to:

- Leaving employment.
- End of contract.
- Completion of a placement.
- Change in responsibilities.
- Leaving the School.

User accounts, data retention and any Grace Period arrangements will be managed in accordance with School procedures and the relevant sections of this policy.

It is the responsibility of users to ensure that important School resources, documents and communications are appropriately transferred before their access is withdrawn.

7. USB Storage, Cloud Storage (OneDrive and Google Drive)

The School has invested in and developed secure network and cloud-based systems to support teaching, learning and professional activities. These systems provide authorised users with secure storage for files, resources and School-related data.

The School maintains approved Microsoft 365 and Google Workspace environments, including OneDrive, SharePoint, Microsoft Teams, Google Drive and Google Classroom, for the storage, sharing and collaboration of educational and business-related information.

Users must not connect USB storage devices, flash drives, portable hard drives or other removable storage media to School computers unless they have received prior written authorisation.

Where authorisation is granted, users must only use the specific devices and media covered by that approval and must ensure that those devices are used solely for the approved purpose.

7.1 USB Exemptions – Requesting Exemption

Requests for exemption from the School's USB storage restrictions should be submitted in writing, including by email, to the Executive Headteacher and the Network Manager. Requests should clearly state the reason for the exemption and the intended use of the device.

Any exemption granted will be subject to the School's discretion and will normally remain in force only until the end of the current academic year. Exemptions will be reviewed annually and may be withdrawn at any time if deemed necessary.

Users granted an exemption remain responsible for ensuring that approved removable media is adequately protected and used securely.

If a user believes that a USB device or other removable media may contain malicious software, it must not be connected to any School equipment until advice has been obtained from the Technical Support Team. Users are responsible for ensuring that removable media is scanned using reputable and up-to-date antivirus software before use.

7.2 Storage of School Files and Data

All users are responsible for ensuring that their work and School-related files are stored on approved School platforms.

Approved storage platforms include:

- Microsoft 365
 - OneDrive (personal work files)
 - SharePoint (shared departmental and organisational resources)
 - Microsoft Teams (collaborative working and resource sharing)
- Google Workspace
 - Google Drive
 - Google Classroom

The School cannot guarantee the recovery of files or resources that have not been stored on approved School systems.

Staff users must not remove, copy or store data that is confidential, sensitive, personal or potentially damaging to the School on non-approved systems without prior authorisation and a legitimate business need.

Any transfer, storage or sharing of School information must comply with the School's Data Protection Policy, Information Security requirements and applicable legislation.

8. Internet – Internet Filtering

Users must use the Internet responsibly, professionally and in a manner consistent with the values and standards of Robert Clack School.

Users must not access, attempt to access, download, store, transmit, print, display or distribute material that is unlawful, obscene, offensive, abusive, discriminatory or otherwise unsuitable within an educational environment.

Any incidents of cyberbullying, harassment or inappropriate online behaviour will be dealt with in accordance with the School's Anti-Bullying and Disciplinary Policies. Where appropriate, evidence may be retained and shared with relevant authorities as part of an investigation.

The School operates internet filtering and monitoring systems to help safeguard students, comply with legal obligations and protect School systems and users. The School determines which websites and online services are accessible through its network and reserves the right to amend filtering arrangements where necessary.

Users must not attempt to bypass, disable or circumvent any internet filtering, monitoring or safeguarding controls implemented by the School. Accessing, attempting to access, or seeking information on how to bypass such controls may constitute a serious breach of School Policy and may result in disciplinary action.

Users are expected to respect the intellectual property rights of others and comply with copyright legislation. Copyright infringement, plagiarism or the unauthorised use of copyrighted materials will be dealt with in accordance with relevant School policies and applicable legislation.

Users should not engage in any online activity that may compromise their professional responsibilities, the reputation of the School, or the safety and wellbeing of students and colleagues.

The School maintains records of internet usage and web activity for safeguarding, security, compliance and investigative purposes. The School reserves the right to review internet access logs, web history and related records where authorised and legally permissible.

Failure to comply with this section may result in the withdrawal of internet access privileges, disciplinary action or referral to the appropriate authorities where required.

9. Handling Sensitive Information

All users are provided with a School email account (currently Microsoft 365) for the purpose of conducting School business and professional communications. This account may be accessed from authorised locations and devices, subject to compliance with this Policy and any associated School procedures.

School email accounts must be used for all School-related correspondence and professional communications.

Staff must not use personal email accounts for School business, the transmission of School information, or professional correspondence. The use of personal email for School activities creates significant security, safeguarding and data protection risks and is therefore prohibited.

Limited personal use of web-based email services may be permitted, provided it does not interfere with professional responsibilities or breach any School policy.

Confidential, personal or sensitive School information must never be transmitted through personal email accounts. This includes correspondence relating to students, staff, safeguarding matters, personnel matters, social services, external agencies, parent communication or any other official School business.

Official communications intended for students, parents, carers, colleagues, governors, external agencies or other stakeholders must be sent using authorised School systems and School email accounts.

The forwarding of School email to external email accounts, including personal email addresses, is prohibited.

9.1 Professional Conduct

All email communications must be professional, respectful and consistent with the values and expectations of Robert Clack School.

Users must not use email systems to send, receive, store or distribute material that is offensive, abusive, discriminatory, threatening, defamatory, unlawful or otherwise inappropriate within an educational environment.

Any incident involving cyberbullying, harassment or inappropriate electronic communications will be dealt with in accordance with the School's Behaviour, Anti-Bullying and Disciplinary Policies. Evidence may be retained and shared with the appropriate authorities where required.

9.2 Cyber Security and Email Safety

Users must exercise caution when handling emails, attachments, hyperlinks and other electronic communications.

Cyber criminals frequently use phishing, impersonation and social engineering techniques to obtain personal information, login credentials, financial information or access to systems. Fraudulent messages may appear to originate from trusted organisations, colleagues or known contacts.

Before responding to any unexpected or unusual request, users should:

- Carefully verify the sender's email address.
- Review the content for unusual language, requests or instructions.
- Exercise caution when opening attachments or selecting links.
- Independently verify requests involving passwords, financial transactions, bank details or sensitive information.
- Contact the sender using a trusted communication method if there is any doubt regarding authenticity.

If an email appears suspicious, users must not reply to it, click links or open attachments until its legitimacy has been confirmed.

Users should remain familiar with current cyber security advice issued by the National Cyber Security Centre (NCSC) and any guidance issued by the School.

9.3 Suspicious, Unsolicited and Malicious Emails

Suspicious, unsolicited, spam or phishing emails must be handled in accordance with current School procedures and cyber security guidance.

Where an email contains threatening, racist, extremist, abusive or otherwise concerning content, the School Senior Leadership Team should be informed immediately. Such emails should be preserved for investigative purposes and should not be deleted unless advised.

Suspicious emails should not normally be forwarded to other users, including Technical Support staff, unless specifically requested as part of an investigation. Where reporting is required, a screenshot and relevant details will usually be sufficient.

9.4 Privacy and Monitoring

Users must not deliberately access, read or interfere with the email correspondence of another person without appropriate authority and lawful justification.

Email communications are generally treated with appropriate privacy and in accordance with applicable legislation. However, the School email system remains the property of Robert Clack School and may be monitored, audited or investigated where authorised and legally permissible.

9.5 Access on Mobile Devices

Staff may access School email and approved Microsoft 365 services using personal mobile devices, smartphones or tablets.

Users choosing to access School systems using personal devices must ensure that:

- The device is not shared with unauthorised individuals.
- Appropriate security controls, including password, PIN, biometric authentication or equivalent protection, are enabled.
- The School is informed promptly if the device is lost, stolen or believed to have been compromised.
- Reasonable steps are taken to protect confidential School information from unauthorised access.

Although the device may be personally owned, use of School systems and data remains subject to this Acceptable Use Policy.

Failure to comply with the requirements of this section may result in disciplinary action and, where appropriate, the withdrawal of access to School systems.

10. Cloud-First Storage

Robert Clack School has a duty to safeguard students, protect School Data, maintain the security of its systems and ensure compliance with legal and regulatory requirements.

To support these responsibilities, the School operates monitoring, filtering and logging systems across its networks, devices, applications and cloud services.

10.1 Purpose of Monitoring

Monitoring may be conducted for purposes including:

- Safeguarding children and vulnerable individuals.
- Protecting School systems and data.
- Detecting cyber security threats and incidents.
- Investigating suspected breaches of School policies.
- Supporting disciplinary, safeguarding or legal investigations.
- Meeting statutory, regulatory and audit requirements.
- Ensuring the effective operation of School systems.

10.2 Systems Subject to Monitoring

Monitoring may apply to any School-owned or School-managed system, including:

- Network activity.
- Internet usage.
- Email communications.
- Microsoft 365 services.
- Google Workspace services.
- Bromcom.

- CPOMS.
- Arbor Finance.
- School devices and laptops.
- Wired and wireless networks.
- Remote access services.
- Cloud-based applications and services.

Monitoring may include activity undertaken both on School premises and when accessing School systems remotely.

10.3 Logging and Audit Trails

The School maintains system logs and audit records to assist with:

- Security monitoring.
- Safeguarding investigations.
- Fault diagnosis.
- Compliance auditing.
- Incident response.

Examples of information that may be recorded include:

- User sign-ins and authentication activity.
- File access and sharing activity.
- Email activity.
- Internet browsing history.
- Security alerts.
- Device activity.
- Administrative actions performed within systems.

10.4 User Expectations

Users should be aware that School systems are provided primarily for educational and professional purposes.

While the School respects individual privacy, users should not expect complete privacy when using School-owned devices, networks or services.

Monitoring will be carried out lawfully, proportionately and only for legitimate business, safeguarding, security or operational purposes.

10.5 Investigations

Where concerns arise regarding:

- Safeguarding.
- Cyber security.
- Data protection.
- Misconduct.

- Unauthorised access.
- Inappropriate use of School systems.

The School reserves the right to investigate relevant activity and review logs, records and other evidence held within School systems.

Investigations will be conducted by authorised personnel and in accordance with:

- UK GDPR.
- Data Protection Act 2018.
- Safeguarding requirements.
- Employment legislation.
- School disciplinary procedures.

10.6 Disclosure of Information

Information obtained through monitoring may be disclosed where:

- Required by law.
- Required by a court order.
- Necessary to protect individuals from harm.
- Required as part of a safeguarding investigation.
- Required by law enforcement or regulatory authorities.
- Necessary for disciplinary proceedings.

Any disclosure will be undertaken in accordance with applicable legislation and School policies.

11. Personal Activities

The Robert Clack School Network, associated digital technologies and online services are provided primarily to support teaching, learning, administration and other legitimate School activities.

Users are expected to use School systems, devices and internet services responsibly, professionally and in a manner consistent with their role and the values of the School.

Limited personal use is permitted provided that such use:

- Does not interfere with teaching, learning or professional responsibilities.
- Does not adversely affect the performance, security or availability of School systems.
- Does not result in additional cost to the School.
- Does not breach any School policy, safeguarding obligation, legal requirement or professional standard.
- Is reasonable, occasional and undertaken during appropriate times.

Personal interests and activities, whilst not discouraged during authorised break periods, must be appropriate for an educational environment and must not be pursued whilst teaching, supervising students or undertaking other duties.

Users must not use School systems for:

- Any unlawful or criminal activity.
- Personal financial gain or commercial activity not authorised by the School.
- Accessing, storing, transmitting or distributing inappropriate, offensive or prohibited material.
- Activities that may bring the School into disrepute.
- Excessive personal use that impacts the user's professional responsibilities or the effective operation of School systems.

The School maintains records of user activity, including internet usage and access logs, for safeguarding, security, compliance and investigative purposes. Where there is reason to believe that School systems have been misused, such records may be reviewed by authorised personnel in accordance with School policies and applicable legislation.

Internet abuse, excessive personal use of School systems, misuse of School resources or other breaches of this Policy may result in disciplinary action. Where unlawful activity is identified, the matter may be referred to the appropriate authorities.

12. Remote Learning, Online Meetings and Digital Collaboration

Robert Clack School supports the use of digital technologies to facilitate teaching, learning, meetings and professional collaboration. All users must maintain the same standards of professionalism, conduct and safeguarding when participating in online activities as would be expected in face-to-face environments.

12.1 Professional Standards

Staff must maintain appropriate professional standards when participating in:

- Remote lessons.
- Virtual meetings.
- Video conferences.
- Webinars.
- Online training sessions.
- Digital collaboration activities.

The standards expected during online interactions are the same as those required when working on School premises.

Users must:

- Conduct themselves professionally and respectfully.
- Follow School policies and procedures.
- Maintain appropriate professional boundaries.
- Use approved School platforms where available.

12.2 Use of Approved Platforms

Remote teaching, meetings and collaboration should be conducted through School-approved platforms and services, including:

- Microsoft Teams.
- Microsoft 365 collaboration services.
- Google Workspace services.
- Other platforms authorised by the School.

The School reserves the right to determine which platforms may be used for educational or business purposes.

12.3 Environment and Presentation

When participating in remote lessons or meetings, users should take reasonable steps to ensure that their environment is suitable and professional.

Staff should:

- Ensure the surroundings are appropriate for a professional or educational setting.
- Minimise distractions where possible.
- Consider the use of background blur or virtual backgrounds where appropriate.
- Ensure confidential information is not visible to unauthorised individuals.
- Dress appropriately and maintain professional standards of appearance.

Particular care should be taken when working from home or in environments where other individuals may be present.

12.4 Safeguarding Requirements

All safeguarding policies remain in effect during remote teaching, learning and communication activities.

Users must:

- Report safeguarding concerns immediately.
- Follow School safeguarding procedures at all times.
- Use only approved communication channels for contact with students.
- Maintain appropriate staff-student boundaries.

Users must not:

- Use personal social media accounts to communicate with students.
- Arrange unofficial online meetings with students.
- Share personal contact details unless explicitly authorised by the School.

12.5 Recording of Lessons and Meetings

Where lessons, meetings or online sessions are recorded, this must be undertaken in accordance with:

- School safeguarding requirements.
- Data Protection legislation.
- The School's Data Protection Policy.
- Any specific guidance issued by the Senior Leadership Team.

Users must not make unauthorised recordings of:

- Lessons.
- Meetings.
- Staff discussions.
- Student activities.

Recordings must be stored only on approved School platforms and retained in accordance with School retention policies.

12.6 Confidentiality

Users must take reasonable precautions to protect confidential information when participating in remote activities.

This includes:

- Preventing unauthorised persons from viewing confidential information.
- Using headphones where appropriate.
- Ensuring sensitive conversations cannot be overheard.
- Securing devices when unattended.

Care should be taken when sharing screens, documents or presentations to avoid the accidental disclosure of personal or confidential information.

12.7 Digital Collaboration

Users are encouraged to collaborate responsibly using School-approved tools.

Communications should be:

- Professional.
- Respectful.
- Relevant to educational or business purposes.
- Consistent with School policies.

The School reserves the right to monitor and audit collaboration platforms in accordance with this policy.

13. Social Networking

Access to social media websites and services is prohibited for staff at Robert Clack School unless there is a legitimate educational, professional or School-related reason for their use.

Users should be aware that many websites and online services are now categorised as social media platforms and may therefore be restricted by the School's internet filtering and safeguarding systems.

Where a member of staff is unable to access a website because it has been categorised as a social media platform, but believes there is a valid educational, professional or operational requirement for access, a request must be submitted to the Senior Leadership Team via:

seniorslt@robertclack.co.uk

The request should clearly outline the website or service required and the educational, professional or business justification for access.

If the request is approved, the Senior Leadership Team will provide written authorisation to the Network Manager instructing that the user's internet access policy be amended accordingly.

Any access granted under this process is provided solely for the approved purpose and may be withdrawn if it is no longer required or if the service is misused.

Users must ensure that any use of social media, whether on School equipment or personal devices, does not compromise their professional responsibilities, the reputation of the School, safeguarding obligations or data protection requirements.

Users must not:

- Publish, share or discuss confidential School information on social media platforms.
- Post content that could reasonably be regarded as offensive, discriminatory, defamatory, inappropriate or damaging to the reputation of the School.
- Represent personal views as those of the School without appropriate authority.
- Engage in online activities that could undermine professional standards, safeguarding responsibilities or public confidence in the School.

For further guidance regarding the use of social media and related applications, users should refer to the Robert Clack School Social Media Policy.

Failure to comply with this section may result in the withdrawal of access permissions, disciplinary action and, where appropriate, referral to the relevant authorities.

14. Safeguarding Issues

14.1 Child Abuse Images (Indecent Images of Children)

An indecent image of a child is any image of a sexual nature depicting a person under the age of 18. The creation, possession, downloading, sharing, printing, storing or distribution of such material may constitute a serious criminal offence under UK law.

If, during the course of your duties, you encounter material that may constitute an indecent image of a child, you must not attempt to investigate the matter yourself.

You must:

- Immediately cease any further activity involving the material.
- Prevent any further viewing of the material where it is safe and appropriate to do so.
- Report the matter immediately to the Designated Safeguarding Lead (DSL) or other appropriate safeguarding personnel.
- Preserve any evidence and follow instructions provided by safeguarding staff.

If such material is displayed on a student's device, the student should be removed from the situation where appropriate and immediate advice sought from safeguarding personnel.

Under no circumstances should any child or young person be shown the image for the purpose of identifying its source, ownership or distribution.

14.2 Adult Pornographic Material

The display of pornographic material within a School environment presents significant safeguarding concerns and may constitute a criminal offence where children are exposed to such content.

If pornographic material is discovered on School systems or devices, users must not attempt to investigate the matter independently. The incident must be reported immediately to the Designated Safeguarding Lead or appropriate safeguarding personnel, who will determine the appropriate course of action.

Users must not show any such material to students or other unauthorised persons, even where the intention is to establish the source of the material or identify those involved.

14.3 Safeguarding Investigations

All investigations concerning indecent images of children, pornography, online safeguarding concerns or other serious safeguarding incidents must be led by designated safeguarding personnel.

ICT Technical Support staff may provide technical assistance where requested but should only become involved under the direction of safeguarding personnel and in accordance with School procedures.

The preservation of evidence, safeguarding of individuals and compliance with legal obligations must take precedence at all times.

Any user who becomes aware of material, behaviour or activity that may pose a safeguarding risk has a duty to report their concerns immediately through the School's safeguarding procedures.

15. Working Away From School

Where staff are authorised to work away from School premises, including working from home, hybrid working or working at alternative locations, they remain fully bound by the requirements of this Acceptable Use Policy and all related School policies.

Failure to comply with these requirements may result in data breaches, cybersecurity incidents, reputational damage to the School and disciplinary action.

15.1 Security and Privacy

Users working remotely must ensure that appropriate security measures are maintained at all times.

- School work should only be undertaken on a device that is not accessible to unauthorised individuals. Users should avoid working on devices shared with family members or other third parties.
- Where a dedicated device is required to perform School duties securely, staff should discuss their requirements with their Line Manager and the School Business Manager.
- Devices used to access School systems must be protected by a strong password, PIN, biometric authentication or equivalent security measure.
- Devices must be locked whenever left unattended.
- Login credentials, authentication codes and Multi-Factor Authentication (MFA) methods must never be shared with another person.
- All School files and work-related documents must be stored only on approved School platforms, including OneDrive, SharePoint, Microsoft Teams and Google Drive.
- School data must not be stored on USB storage devices or other removable media unless specifically authorised.
- Users must take reasonable steps to prevent unauthorised individuals from viewing School information displayed on screens or documents.
- Devices must never be left unattended in public places where they may be lost, stolen or accessed by unauthorised persons.

Any device used to access School systems or process School information, whether School-owned or personally owned, that is lost, stolen or believed to have been compromised must be reported immediately to the School.

15.2 Software and Updates

To reduce the risk of cyber threats and system compromise:

- Operating systems, applications and antivirus software must be kept up to date.
- Users should seek advice from the Technical Support Team if they have concerns about device security or malware protection.
- Unauthorised applications or software must not be installed on School-owned devices.
- Important work files should be stored on approved School platforms to ensure protection and recovery where appropriate.

15.3 Internet Usage

Users must ensure that they use a secure and trusted internet connection when accessing School systems remotely.

- Public or unsecured Wi-Fi networks should be avoided wherever possible.
- Where access from an untrusted network is unavoidable, users should take appropriate steps to protect School information and follow current School guidance regarding secure remote access.

15.4 Work Environment and Equipment

Users should take reasonable steps to create a safe and suitable working environment.

- Screens should be positioned to minimise the risk of unauthorised viewing.
- Appropriate furniture and equipment should be used where possible.
- Regular breaks should be taken to reduce eye strain and fatigue.
- Any hardware, software or technical issues should be reported promptly through the designated Helpdesk system.

15.5 Data Protection

All work undertaken away from School must comply with the UK GDPR, the Data Protection Act 2018 and the School's Data Protection Policy.

Users must:

- Avoid printing confidential or sensitive documents unless there is a clear operational requirement.
- Store and dispose of paper records securely.
- Immediately report any suspected data breach, loss of information or cybersecurity incident.
- Take reasonable steps to ensure that confidential information is not viewed, accessed or disclosed to unauthorised individuals.

Failure to comply with these requirements may result in disciplinary action and, where appropriate, referral to the relevant authorities.

16. School Loaned Computer Equipment

All ICT equipment, devices and associated technology loaned by the School remain the property of Robert Clack School and must be used in accordance with this Acceptable Use Policy, the School's Social Media Policy and any other relevant School policies and procedures.

School-issued devices are provided primarily to support professional duties, teaching, learning and other authorised School activities. Users are expected to take reasonable care of any equipment entrusted to them and to use it responsibly and securely at all times.

Any laptop, computer, tablet or other device loaned by the School is supplied solely to support the user's professional responsibilities. Users should be aware that significant personal use of School loaned equipment may have implications under HM Revenue & Customs (HMRC) rules relating to employee benefits. Where such use may arise, staff should inform the School Business Manager for advice.

Users must:

- Take reasonable precautions to prevent loss, theft, damage or unauthorised use of School equipment.
- Ensure that School devices are protected when used away from School premises.
- Report the loss, theft, damage or suspected compromise of any School device immediately.
- Comply with all School security requirements, including password, authentication and software update requirements.
- Not install unauthorised software or applications on School-owned devices without approval.

School loaned equipment must not be removed from School premises unless it has been appropriately security marked, recorded on the School Asset Register and formally authorised for off-site use.

Users remain responsible for any equipment loaned to them until it has been returned to the School and formally removed from their responsibility in accordance with School procedures.

Failure to comply with this section may result in the withdrawal of equipment, disciplinary action and, where appropriate, recovery of costs associated with loss, damage or misuse.

17. Leaving Robert Clack School

17.1 User Accounts and Access to School Systems

Access to School systems, including Microsoft 365, OneDrive, SharePoint, Microsoft Teams, Google Workspace, Google Classroom and School email services, will remain active until the user's official leaving date.

Following removal from the School's workforce records, user accounts will normally be automatically deactivated. This process typically occurs during the evening of the employee's official leaving date. Staff should therefore ensure that any necessary arrangements relating to files, teaching materials, communications and departmental resources are completed prior to their departure.

Staff members who use Google Classroom, Microsoft Teams or other collaborative platforms are responsible for ensuring that ownership of resources, classes, shared files and other materials required by students or colleagues is appropriately transferred before their leaving date.

Where assistance is required, users should consult their Line Manager and the Technical Support Team well in advance of leaving.

17.2 School Information and Intellectual Property

While many resources contained within a user's personal workspace may have been developed by the individual during their employment, certain documents, information, resources and records may constitute School property and must not be removed, copied or transferred without appropriate authorisation.

Users who are uncertain whether information constitutes School property should seek advice from their Department Leader or Line Manager before removing or transferring any data.

All staff remain bound by confidentiality, data protection and safeguarding obligations after their employment ends.

17.3 Departmental Handover

Once accounts have been deactivated, access cannot normally be granted to other members of staff for the purpose of accessing email, OneDrive, Google Workspace or other personal user accounts, except where lawful and authorised procedures apply.

Staff are therefore strongly advised to:

- Transfer important departmental resources before leaving.
- Share relevant teaching and curriculum materials where appropriate.
- Forward or appropriately redirect important business correspondence.
- Complete handover arrangements with colleagues and Line Managers.

Failure to undertake appropriate handover arrangements may result in the loss of access to important information and resources required by the School.

17.4 Grace Period Following Departure

In exceptional circumstances, a one-off grace period of up to sixty (60) days may be granted to allow continued access to selected School cloud applications following a user's official leaving date.

A grace period may be appropriate where an extended handover process is required or where there is an agreed operational need.

Requests for a grace period must:

- Be made in writing to the School HR Officer.
- Be submitted well before the official leaving date.
- Receive approval from the School.

A grace period cannot be requested or activated after a user has officially left the School.

Where approved, access will normally be limited to teaching and learning systems, cloud services and email. Access to the Management Information System (MIS), finance systems and other restricted applications will normally be withdrawn on the official leaving date unless separate arrangements have been agreed.

At the conclusion of the approved grace period, accounts will be automatically closed. This process is final and cannot normally be reversed.

Users granted a grace period remain fully bound by this Acceptable Use Policy until all access has ceased.

17.5 Return of School Equipment

Staff who have been issued with School-owned ICT equipment, including laptops, tablets, mobile devices, accessories or other technology assets, must return all such equipment before leaving the School unless alternative arrangements have been formally agreed.

Equipment should be returned in good condition, subject to reasonable wear and tear, and any School loan agreements must be formally signed off as complete.

Users should remove any personal files and information before returning equipment. School data and resources must not be deleted, altered or removed prior to return.

Any request to retain School-owned equipment following departure must be discussed and agreed with the School Business Manager before the leaving date.

17.6 Failure to Comply

Failure to comply with the requirements of this section may result in delays to the leaving process, the loss of access to School resources, recovery action relating to School property, or other action deemed appropriate by the School.

18. Closing Statement

Robert Clack School is committed to providing a safe, secure and effective digital environment that supports teaching, learning, safeguarding and the professional activities of all users.

The responsible use of technology is essential in protecting students, staff, School information and School systems from harm. All users are expected to act responsibly, exercise good judgement and comply with the requirements set out in this Acceptable Use Policy and related School policies.

By accessing or using School systems, devices, networks, applications or data, users acknowledge their responsibility to:

- Protect School information and resources.
- Maintain appropriate standards of conduct.
- Support safeguarding and online safety.
- Comply with legal and regulatory requirements.
- Report security, safeguarding or data protection concerns promptly.

The School reserves the right to amend this Policy at any time in response to changes in legislation, safeguarding requirements, cyber security risks, operational needs or technological developments.

This Policy should be read in conjunction with the School's:

- Data Protection Policy
- Safeguarding and Child Protection Policy
- Online Safety Policy
- Social Media Policy
- Staff Code of Conduct
- Remote Working Policy
- Information Security Procedures

Failure to comply with this Policy may result in the withdrawal of access privileges, disciplinary action and, where appropriate, referral to external agencies or authorities.