READING BLUE COAT

Acceptable Use Policy

Scope

This policy applies to all members of the School community (staff or students) who use school IT systems, as a condition of access. Access to school systems is not intended to confer any status of employment on any contractors.

Online behaviour

As a member of the School community you should follow these principles in all of your online activities:

- The School cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the School community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the School community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact students or parents, and students and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Using the School's IT systems

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.

- Do not attempt to circumvent the content filters or other security measures installed on the School's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the School's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the School monitors use of the School's IT systems, and that the School can view content accessed or sent via its systems.

Passwords

Passwords protect the School's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

Passwords must adhere to the following criteria

- Minimum 8 characters
- An uppercase letter
- A lowercase letter
- A number or special character
- Cannot match a previous password

All staff accounts with access to student and/or sensitive data must be protected by Two Factor Authentication (2FA).

Use of Property

Any property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the IT Services department.

Use of school systems

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and students should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the School's right to monitor and access web history and email use.

Use of personal devices or accounts and working remotely

All official school business of staff must be conducted on school systems, and it is not permissible to use personal email accounts for school business. Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the IT Services department.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the School's policies, including [two-factor authentication, encryption etc.]

Staff are not permitted under any circumstances to use their personal devices when taking images, videos or other recording of any student nor to have any images, videos or other recording of any student on their personal devices. Please read this in conjunction with *Child Protection & Safeguarding Policy* and *Staff Code of Conduct*.

Monitoring and access

Staff, parents and students should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the School where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Any personal devices used by students, whether or not such devices are permitted, may be confiscated and examined under such circumstances. The School may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy, and in particular if there is any reason to suspect illegal activity or any risk to the wellbeing of any person.

The use of Virtual Private Networks (VPNs), mobile hotspots and mobile data to circumvent the School's filtering and monitoring systems is expressly forbidden.

Tracking Devices and Technology

The School is not responsible for individual settings on personal devices, nor for the use of tracking apps/devices for purely personal and domestic purposes.

Use of this technology in the context of school activities is not specifically encouraged but if parents do plan to use it then they should be aware of potential third party privacy considerations and only use it for domestic/personal purposes in respect of their own child and/or their child's belongings.

Compliance with related school policies

To the extent they are applicable to you, you will ensure that you comply with the School's *E-Safety, Digital Communication and Student Device Policy*, *Child Protection & Safeguarding Policy*, *Anti-Bullying Policy*, *Data Protection Policy, GDPR Retention Policy, Privacy Notice* and the *Student Manual*.

Retention of digital data

Staff and students must be aware that all emails sent or received on school systems will be kept in archive whether or not deleted. Email accounts will generally be closed and the contents archived within 1 month of that person leaving the School.

Student Account	Password changed within 7 days of leaving.	• Email/OneDrive backed-up and stored • Account deleted within 4 weeks
Staff Account	Password changed within 7 days of leaving.	• Email/OneDrive backed-up and stored

		• Account deleted within 4 weeks (unless longer access requested).

Any information from email folders that is necessary for the School to keep for longer, including personal information (e.g. for a reason set out in the School Privacy Notice), should be held on the relevant personnel or student file. Important records should not be kept in personal email folders, archives or inboxes, nor in local files. Hence it is the responsibility of each account user to ensure that information is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the School's email deletion protocol.

If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact Barry Hines, Head of IT Services (bjh@rbcs.org.uk).

Breach reporting

The law requires the School to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the School regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the School's systems, e.g. through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The School must generally report personal data breaches to the ICO without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the School must keep a record of any personal data breaches, regardless of whether they need to notify the ICO.

If either staff or students become aware of a suspected breach, they must report it immediately to the Data Protection Co-Ordinator (the Bursar).

Data breaches will happen to all organisations, but the School must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and students. The School's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

Use of Artificial Intelligence

Any usage by students of generative AI tools such as Copilot is only permitted in the circumstances outlined in the *AI Policy*, where usage rules, protocols, etc are outlined, and subject to any conditions imposed by that policy. The key points are:

1. Copilot is the ***only*** generative AI tool authorised for use by students and staff at Reading Blue Coat. Students and staff are not permitted to use other generative AI tools, such as Google's Gemini and OpenAI's ChatGPT, without first seeking permission from the Designated Safeguarding Lead and IT Services & Support Manager.
2. ***Only*** students in Years 9-13 are permitted to used Copilot. Students in Years 7-8 are not permitted to use generative AI tools.

Personal or confidential information should not be entered into generative AI tools. This technology can potentially store and/or learn from data inputted and you should consider that any information entered into such tools is released to the internet.

It is also important to be aware that the technology, despite its advances, still produces regular errors and misunderstandings and should not be relied on for accuracy. In particular, students should not use these tools to answer questions about health, medical or wellbeing issues, or indeed anything of a personal nature. It is always best to seek help and recommendations as to reliable resources from the Designated Safeguarding Lead or IT Services & Support Manager.

Breaches of this policy

A deliberate breach of this policy by staff or students will be dealt with as a disciplinary matter using the School's usual applicable procedures. In addition, a deliberate breach by any person may result in the School restricting that person's access to school IT systems.

If you become aware of a breach of this policy or the *E-Safety, Digital Communications and Student Device Policy*, or you are concerned that a member of the School community is being harassed or harmed online you should report it to the Designated Safeguarding Lead. Reports will be treated in confidence wherever possible.

Author(s):	Guy Williams (Deputy Head [Pastoral])
Date:	September 2025
Review Frequency:	Biennial
Next Review Date:	June 2027
Related Policies:	• Artificial Intelligence • Anti-Bullying • Child Protection & Safeguarding • Data Protection • E-Safety, Digital Communications and Student Device • GDPR Retention • Staff Code of Conduct • Use of Generative AI in Academic Work
Agreed by:	 Clare Freeman (Safeguarding Governor) *on behalf of the Full Governing Board*
Date of Agreement:	September 2025