SINCE 604 AD

KING'S SCHOOL

ROCHESTER

IT Acceptable Use Policy

for Staff and Pupils

This policy was adopted on:	10.01.24
The policy was last reviewed on:	24.08.25
Person/Body reviewing:	CFW
Date of next review (except in the case of relevant legislation):	24.08.26

Contents

1. Scope of this Policy

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

2. 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 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, including harmful or inappropriate content such as misinformation, disinformation, conspiracy theories, or material designed to manipulate beliefs or behaviours. Be aware of commercial risks online, including scams, hidden advertising, and manipulative online content (for example, obscene content that promotes violence, discrimination, or extremism or raises safeguarding issues). If staff become aware that pupils are sharing misinformation or harmful conspiracy material, they should report this as a safeguarding concern to the DSL.
- Respect the privacy of others. Only share photos, videos, contact details, or other information about school community members, even if the content is 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, damage, interfere with, gain unauthorised access to others' computer systems, or carry out illegal activities.
- Staff should refrain from using their personal non-school email or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the staff's personal non-school email addresses or social media accounts.

3. Using the school's IT systems

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

- You can only access school IT systems using your 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 or 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.
- Use the school's IT systems to uphold the principles of online behaviour set out above.
- Remember that the school monitors the use of its IT systems and can view content accessed or sent via its systems.

4. 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 should not be the same as your widely used personal passwords.
- You should not let anyone else know your password, nor should you keep a list of passwords where they may be accessed. You must change it immediately if it appears to be compromised.
- You should not attempt to gain unauthorised access to anyone else's computer or confidential information to which you do not have access rights.

5. Cybersecurity and Digital Hygiene

All staff, pupils, and parents/carers have a responsibility to help keep the school's digital systems safe and secure. Good cyber hygiene reduces risks to personal data, safeguarding, and teaching and learning.

Expectations:

- Multi-Factor Authentication (MFA) must be enabled where available.
- Devices and software (school and personal, where used for school purposes) must be kept up to date with the latest security updates.
- Phishing and suspicious activity: all users must be vigilant and report any suspicious emails, links, or system activity immediately to IT or the DSL.
- Storage and transfer of data must only take place on school-approved systems (e.g. Google Workspace). USB drives or personal cloud accounts must not be used.
- Circumventing security controls (including firewalls, filtering, or monitoring) using VPNs, proxies, or other tools is strictly prohibited.
- Lost or stolen devices must be reported to IT immediately so that security measures can be applied.
- Any cyber incident that may compromise security, data, or safeguarding must be reported without delay.

Failure to follow these rules may result in disciplinary action and, where relevant, may also be treated as a safeguarding matter.

6. Use of Property

Any property belonging to the school should be treated with respect and care and used only by those trained and policy-provided. You must promptly report any faults or breakages to the IT & Digital Services team.

7. 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 pupils should keep their personal, family, and social lives separate from their school IT use and limit any personal use of these accounts as much as possible. Again, please know the school's right to monitor and access web history and email use.

8. Use of personal devices or accounts and working remotely

All official school business of staff and governors must be conducted on school systems, and using personal email accounts for school business is not permissible. 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 Director of Digital Strategy / Senior Leadership Team.

Where permission is given for personal devices, these must be subject to appropriate safeguards. Where personal devices are connected via mobile data rather than school Wi-Fi, filtering and monitoring will not apply; users must be aware of and avoid unfiltered access to harmful or inappropriate content in line with the school's policies, including connection to the school's filtered and monitored WiFi connection as the primary data communication method.

9. Monitoring and Access

Staff, parents, and pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct, and performance purposes. Monitoring is a safeguarding duty under KCSiE, not surveillance. Filtering and monitoring cover all required categories, including child sexual abuse material (IWF list), unlawful terrorist content (CTIRU list), adult content, online fraud, violence, extremism/radicalisation, hate speech, self-harm/suicide content, and abuse. IWF and CTIRU blocklists cannot be disabled. The system is reviewed annually, with weekly log reviews and real-time alerts for high-risk content (including through school Wi-Fi) will be monitored for safeguarding, conduct, and performance purposes. The school may access web history and school email accounts where necessary for a lawful purpose, including serious conduct or welfare concerns, extremism, and the protection of others.

Any personal devices used by pupils, whether or not such devices are permitted, may be confiscated and examined under such circumstances. The school might require staff to conduct searches of their 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.

10. 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 explicitly encouraged. Suppose parents/guardians do plan to use it. In that case, they should be aware of potential third-party privacy considerations and only use them for domestic/personal purposes regarding their child and/or their child's belongings.

11. Compliance with related school policies

To the extent they apply to you, you will ensure that you comply with the school's Online Safety, Retention of Records, Email Retention, Safeguarding, Anti-Bullying, and Data Protection Policies.

12. Retention of digital data

Staff and pupils must be aware that all emails sent or received on school systems will be routinely deleted after 18 months unless granted longer access for accounts that can show proof of needing to do so/ kept in an archive whether or not deleted. Email accounts will generally be closed, and the contents irretrievably deleted within 3 months of that person leaving the school.

Any information from email, digital storage or online folders 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 pupil file. Vital records should not be kept in personal email folders, archives, inboxes, or 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 critical information would be lost due to 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 the Director of Digital Strategy.

13. Breach reporting

The law requires the school to notify the authorities and, in some cases, those affected by personal data breaches if they are likely to cause harm. A personal data breach is a security breach leading to the accidental or unlawful destruction, loss, alteration, or 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
- insecure disposal.

The school must generally report personal data breaches to the ICO without undue delay (i.e., within 72 hours), and indeed, if they present 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 we need to notify the ICO. Any breach that may impact a pupil's welfare must be reported to the Designated Safeguarding Lead (DSL) immediately

If either staff or pupils become aware of a suspected breach, contact the Director of Digital Strategy or a member of the Senior Leadership Team as soon as possible.

Data breaches will happen to all organisations, but the school must ensure they are as rare and limited as possible and that, when they do occur, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The school's primary interest and responsibility is to protect potential victims and to have 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 result from a serious conduct issue or breach of policy, but failure to report a breach will be a disciplinary offence.

14. Use of Artificial Intelligence

Generative AI tools will be included in the school's filtering and monitoring risk assessment, and their built-in safety features will be reviewed before use.

Pupils are only permitted to use generative AI tools such as ChatGPT in the circumstances outlined in the school's Use of AI policy. They are subject to any conditions imposed by that policy. Only pupils aged 13 or older may use Generative AI tools like ChatGPT.

Staff must only use **school-approved AI tools** and must ensure **human oversight** of AI outputs before use in lessons/assessments.

All users must **not input personal or sensitive pupil/staff data** into AI tools. Caution should be exercised when entering any information into generative AI tools, which might be used for data harvesting. This technology stores and learns from data inputted, and any information entered such tools is released to the Internet.

It is also important to be aware that despite its advances, technology still produces regular errors and misunderstandings and should not be relied on for accuracy. Pupils should not use these tools to answer questions about health / medical / wellbeing issues or, indeed, anything of a personal nature. It is always best to seek help and recommendations regarding reliable resources from a member of staff / DSL.

15. Use of Google Workspace for Education

By holding a school account, all pupils, staff, and other authorised users consent to the school enrolling them in Google Workspace for Education and its associated services. Users acknowledge that their data will be processed in accordance with Google's Workspace for Education licensing terms and conditions. The school's primary email system will be Gmail, the primary file storage system will be Google Drive, and the primary Virtual Learning Environment (VLE) will be Google Classroom. Additional Google services may be enabled or disabled at the discretion of the Director of Digital Strategy (DoDS) and the Senior Management Team (SMT) as required for individual users or groups.

16. Breaches of this policy

A deliberate breach of this policy by staff or pupils 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.

Suppose you become aware of a breach of this policy or the Online Safety Policy or are concerned that a school community member is being harassed or harmed online. In that case, you should report it to the DSL/Principal. Reports will be treated in confidence wherever possible.

17. Acceptance of this policy

Please confirm that you understand and accept this policy by completing the Google Form relating to your role within the school.

A. Staff/Volunteer

Introduction

This agreement sets out the expectations for staff use of school IT systems, digital platforms, and AI tools. By submitting, you acknowledge you have read and will follow the rules.

Key Points

- I will use strong passwords and enable MFA where available.
- I will keep school devices/software updated and report suspicious activity or phishing emails immediately.
- I will only use school systems (Google Workspace, email) for school business.
- I will not attempt to bypass filters or security controls (VPNs, proxies, etc.).
- I will only use school-approved AI tools, never input personal/sensitive data, and always check outputs.
- I understand all use is monitored for safeguarding purposes.
- I will report online safety concerns via CPOMS to the DSL immediately.

Acknowledgement (required checkbox)

☑ I confirm I have read and understood the Staff Acceptable Use Agreement and agree to follow it.

B1. For pupils (aged 12 and older)

Introduction

This agreement sets out the expectations for staff use of school IT systems, digital platforms, and AI tools. By submitting, you acknowledge you have read and will follow the rules.

Key Rules

- I will use technology responsibly for learning.
- I will not attempt to bypass school filters or use VPNs/proxies.
- I will not share personal information online or misuse social media.
- I will treat others with respect online and never bully, harass, or share harmful content.
- I will not misuse AI tools (e.g. to complete assessments, or by entering personal data).
- I understand school systems are monitored for safeguarding.

- I will report anything unsafe or worrying to a teacher or the DSL.

Acknowledgement (required checkbox)

☑ I have read and understood the Pupil Acceptable Use Agreement and will follow it.

B2. For pupils (aged 11 and younger)

Introduction

This agreement sets out the expectations for staff use of school IT systems, digital platforms, and AI tools. By submitting, you acknowledge you have read and will follow the rules.

Key Rules

- I will use school devices for learning only.
- I will be kind and respectful online.
- I will not share personal details (like my password, address, or phone number).
- I will not try to use websites or games I know I'm not allowed to.
- If I see something upsetting or worrying, I will tell an adult straight away.
- I understand my online activity is checked to help keep me safe.

Acknowledgement (required checkbox)

☑ I will follow these rules when I use technology at school.

Parent Confirmation (required checkbox)

☑ I confirm that I have read and explained these rules to my child, and that they understand them

C. For parents/guardians

Introduction

This agreement sets out the expectations for staff use of school IT systems, digital platforms, and AI tools. By submitting, you acknowledge you have read and will follow the rules.

Key Points

- I understand the school provides filtered and monitored internet access for safeguarding.
- I will support the school by reinforcing online safety rules at home.
- I will not attempt to bypass school systems on my child's behalf.
- I understand that pupils under 13 may only use AI tools under staff guidance.
- I will model respectful online behaviour in my own communication with the school community.

- I consent to my child using the school's online systems (Google Workspace, filtered internet, etc.) as part of learning.

Acknowledgement (required checkbox)

☑ I have read the Parent/Carer Acceptable Use Agreement and agree to support the school in promoting safe and responsible technology use.