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:	27.08.26
Person/Body reviewing:	CFW - Director of Digital Strategy
Date of next review (except in the case of relevant legislation):	01.09.27

Contents

1. Scope of this Policy

This policy applies to all pupils, staff, governors, volunteers, contractors and other authorised users who access King's School Rochester digital services, school-owned devices, accounts, networks or internet connectivity. It also applies to personally owned devices when they are used for school purposes or connected to the School network.

The policy covers use on and off the School site where a school account, school-managed device or school data is involved. Access to School systems is provided for educational and operational purposes and may be withdrawn or restricted where this policy is not followed.

2. Responsible online behaviour

All members of the School community are expected to behave online with the same standards of respect, honesty and responsibility that apply face-to-face.

Do not create, access, send or share illegal, abusive, discriminatory, sexually inappropriate, threatening, extremist or otherwise harmful content.

Do not use technology to bully, harass, intimidate, impersonate, exclude or deliberately embarrass another person.

Treat misinformation, disinformation, scams, manipulated media and AI-generated content critically. Staff must report material that raises a safeguarding concern to the Designated Safeguarding Lead (DSL).

Respect privacy. Images, recordings, contact details, personal information and school information must only be shared through authorised channels and where there is a legitimate reason to do so.

Respect copyright, licensing and intellectual property. Do not present another person's work, including AI-generated work, as your own where this would be misleading or academically dishonest.

Staff must use School-approved communication channels when communicating with pupils or parents and must not use personal email or personal social-media accounts for those communications except in a genuine emergency and in accordance with safeguarding procedures.

3. Using the School's IT systems

School IT systems include, but are not limited to, School accounts, Google Workspace for Education, Microsoft 365 and Entra ID services, managed devices, Wi-Fi, internet access, printing, management systems, cloud services and other applications approved by the School.

Use only the account issued to you. Do not allow another person to use your account or authentication method.

Access only information and systems that you are authorised to use. Attempting to gain additional privileges or access another user's data is prohibited.

Do not deliberately interfere with School systems, networks, devices, security controls or the availability of services.

Software, browser extensions, configuration profiles and applications may only be installed on managed School devices where permitted by IT & Digital Services or through an approved management platform.

Do not connect unauthorised network equipment, access points, routers or storage devices to the School network.

Visitors, contractors and other authorised third parties must use the network access provided or approved for them and must not connect equipment directly to the School's internal network unless authorised by IT & Digital Services.

4. Passwords, authentication and account security

Users are responsible for protecting their School accounts and authentication methods.

Use a strong, unique password or passphrase and do not reuse a School password for personal services.

Never share passwords, verification codes, security keys or MFA prompts. IT staff will not ask you to disclose your password.

Multi-factor authentication (MFA) is mandatory for staff accounts accessing cloud services and for privileged or IT administrative accounts. It must also be used for other accounts where required by the School. Users must not approve an MFA request they did not initiate.

Do not approve an MFA prompt you did not initiate. Unexpected prompts, account lockouts or suspected compromise must be reported immediately to IT & Digital Services.

Passwords must be changed promptly where compromise is suspected or when directed by the School.

5. Cybersecurity and digital hygiene

Cybersecurity is a shared responsibility. Good digital hygiene protects teaching and learning, personal data, safeguarding information and the School's operations.

Report phishing, suspicious links, unusual login activity, malware warnings or other suspected cyber incidents promptly to IT & Digital Services.

Keep personally owned devices used for School purposes supported and up to date. School-managed devices will receive updates and security settings through the appropriate management platform.

Devices must be locked whenever they are left unattended, including on School premises, and users must take reasonable steps to prevent confidential information being viewed by unauthorised people.

Store School information only in approved School systems. Personal cloud storage, personal email and unapproved file-transfer services must not be used for School data.

Removable storage should only be used where specifically required and authorised. Sensitive or personal data must not be stored on an unencrypted removable device.

Do not disable or attempt to bypass antivirus, device management, certificates, filtering, firewall, access-control or other security measures.

Lost or stolen School devices, or personal devices containing School data, must be reported immediately so that protective action can be taken.

6. School-provided devices and property

School-provided devices and accessories remain School property unless expressly transferred under a separate agreement. They must be treated carefully, kept secure and used in accordance with any device-specific agreement.

The School's 1:1 environment includes managed iPads, Windows devices and Chromebooks. Where a pupil cohort has been issued a particular School device for classroom use, that device is the expected classroom device unless an agreed reasonable adjustment or other authorised exception is in place.

Do not remove management profiles, security certificates, restrictions or School configuration from a managed device.

Do not deliberately damage, mark or modify devices or accessories.

Faults, damage, loss or theft must be reported promptly through the School's normal IT support or device-loan/repair process.

School devices may be reset, remotely managed, locked or wiped where necessary for security, safeguarding, maintenance or reassignment.

7. School accounts, email and cloud services

School email, Google Workspace, Microsoft 365 and other authorised cloud services are provided for education and School business. Reasonable incidental personal use by staff should be limited and must not interfere with duties, security, storage or safeguarding requirements.

Official School business must be conducted using School-approved accounts and services rather than personal email or personal cloud accounts.

Google Workspace for Education is the School's primary collaboration environment, including Gmail, Google Drive and Google Classroom. Microsoft services are also used where required for identity, licensing, device management and authorised applications.

Shared Drives and other shared repositories should be used for records that belong to a team, department or the School rather than an individual. Access must follow least-privilege principles and should be reviewed when roles change.

Users must take care when sharing files or adding external collaborators and must check that the intended recipient has the appropriate access.

8. Personal devices, BYOD and remote working

The School permits personally owned devices in defined circumstances. This includes the Sixth Form BYOD model and authorised staff use. Use of a personal device does not reduce the user's responsibilities for safeguarding, data protection, confidentiality or cybersecurity.

Sixth Form pupils participating in BYOD must use a device that meets the School's published minimum specification and must complete any required onboarding, including connection to the approved BYOD Wi-Fi and installation of the School security certificate or profile where required.

While on the School site, authorised personal devices used for learning or School business should use the School's approved Wi-Fi rather than mobile data or a personal hotspot.

Using mobile data, a hotspot, VPN, proxy, private relay or similar technology to evade School filtering, inspection or access controls is prohibited.

Users must not remove or deliberately interfere with certificates or configuration required for secure access to School services.

School data should not be downloaded or synchronised to a personal device unless there is a legitimate School purpose and appropriate safeguards are in place.

Remote working must use School-approved accounts, systems and storage. Users should work in a way that prevents confidential information being viewed or overheard by unauthorised people.

9. Filtering, monitoring and network security

The School provides filtered internet access as part of its safeguarding and cybersecurity arrangements and in line with current statutory guidance and the Department for Education filtering and monitoring standards.

School internet traffic is filtered using Smoothwall. HTTPS inspection and the School security certificate are used where configured and appropriate so that encrypted web traffic can be filtered effectively. Managed devices receive the required configuration through their management platform; authorised BYOD users may be required to install a certificate or profile as part of connection to the network.

Internet and network activity may be logged and reviewed for safeguarding, security, operational and lawful investigative purposes. Automated alerts may be generated for specified high-risk activity.

Filtering and monitoring are proportionate controls; they do not mean that every screen, message or action is continuously watched by a member of staff.

The School may block websites, applications, categories, protocols or services where necessary for safeguarding, security, legal compliance, bandwidth management or teaching and learning.

Users must not attempt to test, evade, disable or circumvent filtering or monitoring controls without explicit authorisation from IT & Digital Services for a legitimate technical purpose.

Where a device uses mobile data or another network outside the School's control, School network filtering may not apply. Pupils must not use this as a means of bypassing School controls while on site.

Any safeguarding concern identified through digital activity must be handled in accordance with the Safeguarding and Child Protection Policy and referred to the DSL. Technical logs and other digital evidence will only be accessed or retained where there is a legitimate and lawful reason.

10. Search, access and examination of devices

The School may inspect School-owned devices, School accounts and School systems where necessary for safeguarding, cybersecurity, maintenance, legal compliance or the investigation of a suspected policy breach. Access will be proportionate and limited to what is reasonably necessary.

Searching or examining a pupil's personally owned device must be carried out only where permitted by law and School policy, including the Behaviour Management and Safeguarding policies. Staff should not conduct ad-hoc searches of personal devices or personal accounts outside those procedures.

11. Tracking devices, location services and connected technology

The School is not responsible for personal tracking applications, smart tags or location services used by families for domestic purposes. Such technology must not be used in a way that compromises the privacy, safety or dignity of other members of the School community.

Users must not attach tracking or recording technology to another person or their belongings without lawful authority and appropriate consent. School-managed location or device-management functions may be used for legitimate security, safeguarding, loss-prevention or asset-management purposes.

12. Retention and management of digital information

Email and digital records must be managed in accordance with the School's Email Use & Retention Policy, Records Retention arrangements, Data Protection policies and any applicable safeguarding or legal requirements. This policy does not set a separate retention period.

Email should not be used as the sole long-term record of important School information. Records that must be retained should be transferred to the appropriate School system, Shared Drive, pupil/staff record or other authorised repository.

Users must not keep unnecessary copies of personal or confidential information in local downloads, personal folders or duplicate cloud locations.

When a member of staff or pupil leaves, access to accounts and data will be handled under the School's leaver, retention and account-closure procedures.

Advice on appropriate storage or retention should be sought from the Director of Digital Strategy, Data Protection Officer or relevant information owner.

13. Data breaches and cyber-incident reporting

A personal data breach or cyber incident includes accidental or unlawful loss, destruction, alteration, disclosure of or access to personal data, as well as security incidents that may threaten School systems or safeguarding information.

Examples include a lost device containing School data, a compromised account, malware, accidental oversharing of a file, a misdirected email, inappropriate permissions, insecure disposal or unauthorised access.

Suspected incidents must be reported immediately to the Director of Digital Strategy / IT & Digital Services and, where personal data is involved, to the Data Protection Officer in accordance with the School's breach procedure.

Where an incident may affect a pupil's welfare or involves harmful online content, it must also be reported to the DSL without delay.

The School will assess incidents and make any required notifications to the Information Commissioner's Office or affected individuals within the applicable legal timescales. Users must not conceal an incident or attempt to investigate a suspected breach in a way that could destroy evidence.

14. Use of Artificial Intelligence

Artificial intelligence, including generative AI, can support learning and productivity when it is used safely, ethically and transparently. Use must follow the School's AI guidance/policy, assessment rules, safeguarding expectations and the terms and age requirements of the relevant service.

Only School-approved AI services may be used with School accounts or for processing School information.

Personal, confidential, safeguarding, special-category or otherwise sensitive School data must not be entered into a public or unapproved AI service.

AI output must be checked by a human for accuracy, bias, suitability, copyright and safeguarding concerns before it is relied upon or shared.

Pupils must follow teacher instructions about whether and how AI may be used in a task or assessment and must acknowledge AI assistance where required.

AI must not be used to impersonate others, create harmful or sexualised content, generate deceptive material, bypass academic rules, or make high-impact decisions about individuals without appropriate human oversight.

AI services may be included in the School's filtering and monitoring risk assessment, and access may be restricted by age, user group or service where appropriate.

15. Google Workspace for Education and other managed platforms

School accounts may provide access to Google Workspace for Education and other approved services needed for teaching, learning and administration. Gmail is the School's primary email platform, Google Drive is the primary collaborative file-storage environment, and Google Classroom is the primary virtual learning environment unless the School specifies otherwise for a particular purpose.

Additional services may be enabled, restricted or disabled for particular users or age groups. Access is managed centrally and may change to meet safeguarding, licensing, security, curriculum or

operational requirements. Users must comply with School instructions and the applicable terms of service.

16. Breaches of this policy

Breaches may result in restriction or withdrawal of access, removal of a device from the network, disciplinary action under the relevant staff or pupil procedure, a requirement to repair or replace damaged equipment, or referral under safeguarding, data-protection or legal procedures as appropriate.

Accidental mistakes should be reported promptly so that harm can be limited. Deliberately concealing an incident, bypassing controls, accessing information without authorisation or knowingly placing others or School systems at risk will be treated more seriously.

Concerns about harmful online behaviour, cyberbullying or safeguarding must be reported to an appropriate member of staff and, where required, recorded through the School's safeguarding procedures. Technical faults and cybersecurity concerns should be reported to IT & Digital Services through the approved support route.

17. Acceptance of this policy

Users may be required to confirm that they have read, understood and will follow this policy and the appropriate Acceptable Use Agreement for their role. The School may use an electronic acknowledgement, including a Google Form, to record acceptance.

A. Staff and volunteers

By accepting this agreement, I confirm that I understand the expectations for my use of School IT systems, accounts, devices, digital platforms and AI tools.

Key commitments

I will protect my account, use MFA when required and report suspicious activity promptly.

I will use School-approved accounts, storage and communication channels for School business.

I will protect personal and confidential information and will not place sensitive School data in unapproved cloud or AI services.

I will not bypass filtering, certificates, device management or other security controls.

I understand that relevant system and network activity may be logged and reviewed for safeguarding, security and lawful operational purposes.

I will report safeguarding concerns through the School's safeguarding procedures and cyber/technical incidents to IT & Digital Services.

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

B1. Pupils aged 12 and over

By accepting this agreement, I agree to use School technology responsibly and safely.

Key rules

I will use my School account and device responsibly for learning and School activities.

I will keep my password and authentication details private.

I will not use VPNs, proxies, hotspots, mobile data or other methods to bypass School filters or restrictions while at School.

I will be respectful online and will not bully, harass, impersonate or share harmful or inappropriate material.

I will only use AI when my teacher and School rules allow it, and I will not use it to cheat, impersonate someone or create harmful content.

I understand that activity on School systems and networks may be logged or reviewed to help keep people and systems safe.

I will tell a trusted adult if something online worries me and will report technical or security problems rather than trying to fix or bypass controls myself.

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

B2. Pupils aged 11 and under

These rules help us use technology safely and kindly at School.

Key rules

I will use my School device and account for learning and follow my teacher's instructions.

I will keep my password private.

I will be kind and respectful when I use technology.

I will not try to get around School blocks or settings.

I will not share private information, photographs or recordings unless an adult at School has told me it is safe and appropriate.

If I see something upsetting, unsafe or strange, I will stop and tell an adult I trust.

Acknowledgement: I will follow these rules when I use technology at School.

Parent/carer confirmation: I confirm that I have read and explained these rules to my child and will support the School's expectations for safe and responsible technology use.

C. Parents and carers

By accepting this agreement, I understand the School's expectations for safe and responsible use of its digital services.

I understand that the School provides filtered internet access and uses proportionate logging and monitoring as part of safeguarding and cybersecurity arrangements.

I will support my child in following School rules for devices, accounts, online behaviour, BYOD and AI.

I will not help my child bypass School controls or use mobile data, hotspots, VPNs or similar tools to evade filtering while at School.

I understand that School-managed devices may be remotely configured, managed, locked or reset where necessary.

I understand that personally owned devices used for Sixth Form BYOD must meet the School's requirements and complete the required network/security onboarding.

I will model respectful online communication and will raise concerns through the appropriate School channels.

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