STAHS
PREP SENIOR SIXTH

Acceptable Use Policy (AUP)

Electronic Information & Communications
Policy Related Document

June 2026

THINK BEYOND

P15: Electronic Information and Communications Policy (Related Document)

Acceptable Use Policy

1. Scope of this policy 2
2. Online behaviour 2
3. Using the School's IT systems 2
4. Passwords 2
5. Use of School property 3
6. Use of School systems 3
7. Use of personal devices or accounts and working remotely 3
8. Monitoring and access 3
9. Compliance with related School policies 4
10. Retention of digital data 4
11. Breach reporting 4
12. Breaches of this policy 5
13. Acceptance of this policy 5

1. Scope of this policy

1.1 This policy applies to all members of the STAHS community (including staff, pupils, governors and visitors) 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.

2. Online behaviour

2.1 As a member of the STAHS community, you should follow these principles in all of your online activities, including content created or modified using Artificial Intelligence (AI) tools. Users remain fully responsible for the accuracy, appropriateness and legality of all content they produce.

a) 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.

b) 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, is bullying, or raises safeguarding issues).

c) 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.

d) Do not access or share material that infringes copyright, and do not claim the work of others as your own.

e) 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.

f) Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

1.1. 2.2 Use of Artificial Intelligence (AI)

a) Staff may make use of generative AI tools to assist with administration, lesson planning and educational activities, provided that such use complies fully with this Acceptable Use Policy, the Data Protection Policy, and Safeguarding requirements.

b) Senior School pupils may make use of AI tools which have been approved for their year group, for specified purposes, unless a pupil's parent has opted out of giving permission. The approved tools, specified purposes and year group restrictions are published in toolkits on the staff and pupil dashboards and are updated periodically. Pupils must not create personal accounts on AI platforms unless explicitly approved by the School and compliant with age restrictions.

c) Prep pupils may only use AI in a teacher-led or supervised context using approved tools. Independent or unsupervised use is not permitted.

d) All members of the STAHS community must follow the School's Artificial Intelligence Protocol. You must be ethical in your use of AI, must not use it to generate harmful or biased material, and must not provide an AI tool with any personal, sensitive or identifying information about yourselves, the School, other staff members, pupils or your/their families – e.g. Never type your name, your school, your photo, or any personal information about yourself or others into AI tools. Copyrighted materials, both internal

and external, must not be uploaded into AI models unless the tool has been formally approved by the School and appropriate data protection safeguards are in place

e) Approved AI tools (such as Microsoft Copilot within the School tenant) may be used where data protection, security, and monitoring requirements are met. Use of unapproved tools for School data is prohibited. Where there is any uncertainty about whether a tool is approved, staff must assume it is not approved and seek guidance from IT.

f)

g) You must not pass off AI-generated content as your own and the School prohibits the use of any form of AI in internal assessments and external examinations. For work submitted which contributes towards examinations, such as Non-Examination Assessments (NEAs), pupils and staff must adhere to the JCQ and exam board regulations on AI use.

h) AI must not be used to make safeguarding decisions, behaviour judgements, or any decisions that could impact pupil welfare without appropriate human oversight.

i) The School reserves the right to monitor and restrict the use of AI tools in line with its monitoring, safeguarding and acceptable use requirements.

3. Using the School's IT systems

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

a) Only access School IT systems using your own username and password. Do not share your username or password with anyone else.

b) 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.

c) Do not attempt to install software on, or otherwise alter, School IT systems.

d) Do not use the School's IT systems in a way that breaches the principles of online behaviour set out above.

e) 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.

4. Passwords

4.1 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), 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.

4.2 Many of the School's electronic information and communications systems require two-factor authentication (including the Office 365 suite and CPOMS).

4.3 The School may require you to change your password on any or all School electronic information and communications systems at any time, without notice, and may suspend your access to these systems until your password has been changed.

5. Use of School property

5.1 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 team.

6. Use of School systems

6.1 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 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.

7. Use of personal devices or accounts and working remotely

7.1 All official School business of staff and governors 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 Head of Prep or Head of Senior.

7.2 Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the School's policies, including the School's BYOD guidance.

8. Monitoring and access

8.1 You should be aware that School email, internet usage (including through the School wi-fi) and other online (and in some cases, offline) activity 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.

8.2 Smoothwall Filter by Qoria provides real time, content aware web filtering, dynamically analysing web pages at the point of request to control internet access and block inappropriate or harmful online content, supporting safe and effective digital learning. Qoria Monitor is a real time, human moderated digital monitoring solution operating 24/7/365. It uses advanced behavioural analysis and trained moderators to identify students who may be becoming vulnerable, issuing timely alerts to designated staff to support early safeguarding intervention and promote safer online behaviour. Together, these solutions are designed to support STAHS in meeting KCSIE and Department for Education filtering and monitoring expectations when implemented as part of a wider safeguarding framework.

8.3 Limitations of Monitoring on Personal Devices

While the School employs robust filtering and monitoring systems (including Smoothwall and Monitor) to support safeguarding, these controls are most effective when users are operating on School-managed devices and networks.

Where pupils or staff use personal devices (including BYOD) or access the internet through non-managed connections, the School's ability to monitor activity may be limited to network-level controls such as DNS filtering. In such cases:

The School may not be able to inspect encrypted traffic or monitor content in real time

Some online activity, including the use of certain apps or AI tools, may not be fully visible to monitoring systems

Safeguarding controls may therefore be less comprehensive than on School-managed devices

For this reason:, Use of personal devices is subject to additional restrictions and approval by The Head.

Higher levels of supervision are required where personal devices are used The School may restrict access to certain services or require use of managed devices for specific activities,

8.4 Any personal devices used by pupils, whether or not such devices are permitted, may be confiscated and examined under such circumstances. Further details can be found in the Pupil Behaviour Policy and its related documents.

8.5 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.

9. Compliance with related School policies

9.1 To the extent they are applicable to you, you will ensure that you comply with the School's policies, including the Safeguarding and Child Protection Policy, Pupil Behaviour Policy, Anti-bullying Policy, Teaching, Learning and Assessment Policy, and Data Protection Policy.

10. Retention of digital data

10.1 Staff and pupils must be aware that all emails sent or received on School systems will be archived for a minimum of one year and could be held indefinitely. And email accounts will generally be closed and the contents archived immediately upon that individual leaving the school.

10.2 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 pupil 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.

10.3 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 Head of Prep or Head of Senior.

11. Breach reporting

11.1 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.

11.2 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:

a) Loss of an unencrypted laptop, USB stick or a physical file containing personal data;
b) Any external hacking of the School's systems, e.g. through the use of malware;
c) Application of the wrong privacy settings to online systems;
d) Misdirected post, fax or email;

e) Failing to bcc recipients of a mass email; and
f) Unsecure disposal.

11.3 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 we need to notify the ICO.

11.4 If either staff or pupils become aware of a suspected breach, they should immediately contact the Head of Prep or Head of Senior.

11.5 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 pupils. 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.

12. Breaches of this policy

12.1 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.

12.2 If you become aware of a breach of this policy or the online safety guidance in the School's Safeguarding and Child Protection Policy, or you are concerned that a member of the School community is being harassed or harmed online you should report it to the Head of Senior, Head of Prep, or a Deputy Head. Reports will be treated in confidence wherever possible.

13. Acceptance of this policy

13.1 This policy is communicated to all STAHS pupils annually in an age-appropriate manner through an in-person briefing.

13.2 A copy of the policy, along with any presentation materials shared with pupils, is provided to parents each year.