
Online Safety and Acceptable Use Policy (AUP)

Revision and Terminology

Please refer to the Policies Review Schedule, or in line with any changes in regulations.

Document Title	Online Safety and Acceptable Use Policy
Status of policy	Statutory
Version Number:	2
Author name and role title	Anthony Davies, Bursar
Authorised by	Head of School
Approved by	General Manager/Board of Governors
Effective date of Policy:	22 September 2026
Review Date:	22 September 2027

Contents

1	Purpose and Scope	3
2	Principles	3
3	Legislation and guidance	4
4	Roles and Responsibilities.....	4
5	Unacceptable Use	7
6	Staff (including governors, volunteers and contractors).....	9
7	Access to the internet over Wi-Fi....	12
8	Monitoring and filtering of the school network and use of ICT Facilities.....	12
9	Related Policies.....	13
10	Appendix 1 – Staff agreement with the Acceptable Use Policy	14
11	Appendix 2 – Pupil agreement with the Acceptable Use Policy	15

1. Purpose and Scope

This Online Safety and Acceptable Use Policy (AUP) sets out the expectations for the safe, responsible and lawful use of digital technologies within the School. It applies to:

- 1.1 Students/Pupils.
- 1.2 Teaching and support staff.
- 1.3 Contractors, visitors, volunteers and temporary users.

Our approach to online safety is based on addressing the following 4 categories of risk:

- 1.4 **Content** – being exposed to illegal, inappropriate, or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- 1.5 **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- 1.6 **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending, and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- 1.7 **Commerce** - risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2. Principles

The School is committed to:

- 2.1 Have robust processes in place to ensure the online safety of pupils, staff, volunteers, and governors.
- 2.2 Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- 2.3 Establishing clear mechanisms to identify, intervene and escalate an incident, where appropriate.

3. **Legislation and Guidance**

3.1 This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education \(KCSiE\)](#) and advice for school's on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying \(including cyber\)](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)
- [Protecting learners from radicalisation](#)
- [National Cyber Security Centre \(NCSC\): Cyber Security for Schools](#)

3.2 It reflects existing legislation, including but not limited to:

- [The Computer Misuse Act 1990](#)
- [The Education Act 1996](#)
- [The Education and Inspections Act 2006](#)
- [The Equality Act 2010](#)
- [The Education Act 2011](#)
- [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#) – UK GDPR
- [Education and Training \(Welfare of Children\) Act 2021](#)

3.3 Learners aged 15–18 are naturally curious, and exploring new ideas is a normal part of development. However, when using the school systems, learners are expected to exercise good judgement. A helpful guiding principle is this: only access or search for content that you would feel comfortable viewing with your screen visible to your peers, teachers, or parents. If you would feel the need to hide it, it is likely not appropriate for school networks or devices. This same guiding principle applies to teachers, support staff and contractors.

3.4 Users of the School IT systems, including any devices connected to the school's Wifi networks, such as personal electronic devices and bring your own devices (BYOD), agree to third party blocking, filtering and monitoring as a means of providing safe online access. Monitoring is not constant; it activates only when access to unsuitable material or flagged keywords is detected.

4. **Roles and Responsibilities**

4.1 Board of Governors¹

The Board of Governors has overall responsibility for monitoring this policy and holding the Head of School accountable for its implementation. They will:

- Maintain strategic oversight — Ensuring the school has a comprehensive, up-to-date Acceptable Use Policy (AUP) that aligns with the school's ethos, safeguarding commitments, and long-term digital strategy.
- Ensure legal and regulatory compliance — Confirming that the AUP meets statutory duties, including data protection, safeguarding, online safety guidance, and any relevant inspection frameworks.
- Oversee risk management — Monitoring that appropriate systems, controls, and reporting mechanisms are in place to identify, assess, and mitigate risks related to digital use, cyber security, and student wellbeing.
- Ensure accountability and review — Ensuring regular review cycles, receiving reports from senior leaders on compliance and incidents, and holding the school leadership to account for effective implementation.

4.2 The Head of School

The Head of School is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

4.3 The Designated Safeguarding Leads (DSLs)

The DSL takes lead responsibility for online safety in the school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Senior Leader responsible for IT, the Service provider and other staff, as necessary, to address any online safety issues or incidents.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Working with the Senior Leader responsible for IT to make sure the appropriate systems and processes are in place.

¹ The General Manager, Headquarters staff, and Governors together act as the functional Board of Governors, with ultimate authority vested in the three principal Governors.

- Managing all online safety issues and incidents in line with the school child protection policy.
- Ensuring that any online safety incidents are logged by the school DSLs and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Board of Governors.

4.4 Our ICT Provider

Our ICT provider is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated at least annually with the Senior Leader responsible for IT to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting routine full security checks and monitoring the school's ICT systems.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

4.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Ensuring that they understand and adhere to this policy and ensuring its implementation by others.

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 1) and ensuring that pupils follow the school's terms on acceptable use (appendix 2).
- Working with the DSL to ensure that any online safety incidents are logged by the school and dealt with appropriately in line with this policy.
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

4.6 **Parents and carers**

Parents and carers are expected to:

- Agree to work in partnership with the school to help maintain a safe, respectful and secure online environment for all pupils.
- Support the school's approach to online safety, follow guidance shared by staff, and encourage their child to use technology responsibly at home and in school.
- Communicate promptly with the Head of School or the Designated Safeguarding Lead, if issues arise, so that they can be addressed quickly and constructively.
- If Acceptable Use Policy is breached, agree to cooperate fully with the school to resolve the matter in the best interests of the child.

Parents can access advice and guidance relating to internet usage and keeping their children safe online at [The UK Safer Internet Centre](#) and [Childnet](#).

5. **Unacceptable use**

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 5.3 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright.
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the school's policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Online gambling, inappropriate advertising, phishing and/or financial scams.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful.
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams.
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, its students, or other members of the school community.
- Connecting any device to the school's ICT network without approval from authorised personnel.
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data.
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel.
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities.
- Causing intentional damage to the school's ICT facilities.
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation.
- Using inappropriate or offensive language.
- Promoting a private business, unless that business is directly related to the school.
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms.
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way.
- No work of any kind can be carried out on any school IT hardware, software, systems or infrastructure by anyone other than school IT staff or fully vetted partner IT firms.
- Using AI tools and generative chatbots (such as ChatGPT):

- During assessments, including internal and external assessments, and coursework.
- To write their homework or class assignments, where AI-generated text or imagery is presented as their own work.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

5.2 Exemptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Headteacher's discretion.

Students may use AI tools and generative chatbots:

- As a research tool to help them find out about new topics and ideas.
- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed.

5.3 Sanctions

Students and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's Behaviour Policy or Staff Code of Conduct.

6. Staff (including governors, volunteers, and contractors)

6.1 Access to school ICT facilities and materials

The school's Network Manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices.
- Access permissions for certain programmes or files.

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should notify their Line Manager.

6.2 Use of phones and email

The school provides each member of staff with an email address. This email account should be used for work purposes only. All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents/carers and students, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the bursar immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or students. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters. Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 5.

6.3 Personal use

Staff are permitted to use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Headteacher may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time teaching hours.
- Does not constitute 'unacceptable use', as defined in section 5.
- Takes place when no students are present.
- Does not interfere with their jobs, or prevent other staff or students from using the facilities for work or educational purposes.

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 8). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the Staff Code of Conduct.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where students and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of social media and use of email protect themselves online and avoid compromising their professional integrity.

6.4 Remote access

We allow staff to access the school's ICT facilities and materials remotely. Remote access is provided using school laptops only. It is provided over an encrypted VPN.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the network manager or Headteacher may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

The school's data protection policy can be found on the school website.

7. Access to the internet over Wi-Fi

The school wireless internet connection is secured and has filtering applied to prevent access to unsuitable sites. The school has several WI-FI's for different purposes (such as staff, students & guests) and personnel are only to access Wi-Fi for which they have been granted access. Passwords are not to be shared.

Regardless of which Wi-Fi I is used to access the internet, the school's ICT monitoring activities (see section 8) will continue to operate. Anyone breaching the unacceptable use policy (section 5), should expect to be dealt with in the same manner regarding sanctions, even if accessing over a personal device.

8. Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation
- For Safeguarding of the users

Our governing board is responsible for making sure that the school meets the DfE's. [filtering and monitoring core standards](#) and that:

- Appropriate filtering and monitoring systems are in place.
- Staff are aware of those systems and trained in their related roles and responsibilities.
- For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns.
- It regularly reviews the effectiveness of the school's monitoring and filtering systems.

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place. Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

9. **Related Policies**

- Safeguarding
- Behaviour
- Staff Code of Conduct
- Data Protection

Appendix 1: Staff acceptable use agreement – applies to governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name:	
Organisation:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material). • Use them in any way which could harm the school's reputation. • Access social networking sites or chat rooms in a way that is inconsistent with my professional responsibilities or school policies. • Use any improper language when communicating online, including in emails or other messaging services. • Install any unauthorised software or connect unauthorised hardware or devices to the school's network. If I am in any doubt, I will refer the matter to Aztech. • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its students or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote any private business, unless that business is directly related to the school.	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a Student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that Students in my care do so too.	
Signed:	Date:

Appendix 2: Student acceptable use agreement

Acceptable use of the school's ICT facilities and the internet: agreement for students
Name:
When using the school's ICT facilities and accessing the internet in school, I will not: • Use them for a non-educational purpose during school hours. • Use them without a teacher being present, or without a teacher's permission during school hours. unless this forms part of an authorised independent study period. • Use them to break school rules. • Access any inappropriate websites. • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms except when using school-approved services for educational purposes under teacher supervision. • Open any attachments in emails, or follow any links in emails, without first checking with a teacher, unless the email or link originates from a known and trusted source, such as a member of staff or a school-approved educational service. • Use any inappropriate language when communicating online, including in emails • Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video • Share my password with others or log in to the school's network using someone else's details • Bully other people • Use AI tools and generative chatbots (such as ChatGPT): - During assessments, including internal and external assessments, and coursework - To present AI-generated text or imagery as my own work • Boarders may use social media and messaging services outside school hours to communicate with parents, guardians, family and friends, subject to the school's boarding rules, online safety expectations and any restrictions imposed for safeguarding reasons. • When using social media outside school hours, I will not share personal information that could put myself or others at risk, arrange meetings with people I know only online, or engage in cyberbullying, harassment or any other inappropriate online behaviour. I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed:

Date: