Online Safety Policy (Approved Spring 2025)

Status	Statutory	Date created	November 2022
Any other statutory names for this policy	No	Date first approved	Spring 2023
Responsibility for this policy	DSL	Date last reviewed	Spring 2025
Committee with responsibility for its review	T&L	Frequency of review	Annual
		Website	Yes
Approval necessary	FGB		

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- 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')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- 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
- 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; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- Meeting Digital and Technology Standards in Schools and Colleges
- Education for a Connected World 2020
- DfE guidance on Generative AI Jan 2025

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs (from CPOMS report) as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

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

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented and adhered to consistently throughout the school
- Procuring filtering and monitoring systems
- Documenting decisions on what is blocked and allowed
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged on CPOMS (for Students) and Staff Concerns document (for Staff) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged on our bullying record and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety in staff briefings, bulletins as well as more detailed Inset training. Appendix 4 contains a self-audit for staff on online safety training needs which is completed yearly.
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils and staff are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensure that filtering and monitoring reports are robust and provided to the DSL

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Daily security checks are conducted with a monthly audit of monitoring systems
- Blocking access to potentially dangerous sites whilst in school and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix 2), and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- 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'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum which is audited here:

Curriculum Audit - PSHE, Computing, AI

Guidance on this can be found in the National Curriculum computing programmes of study.

All schools have to teach Relationships and sex education and health education in secondary schools

In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary school, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyberbullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyberbullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / member of the DSL team.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are

images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (see appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them between entering the school gates in the morning and 3.30 pm.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

- Minimising risk of loss or theft by keeping devices secure. All hard drives are encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Using the anti-virus and anti-spyware software which is installed on school devices
- Not installing software themselves. IT will keep operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the IT manager.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The school logs behaviour and safeguarding issues related to online safety on CPOMS. Any online concerns which have been flagged by Smoothwall are tagged accordingly so that we can keep a record.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board. The policy review will be supported by an annual review of AHS practice (Appendix 4) and risk assessment (Appendix 5) that considers and reflects the risks that AHS students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Policies & Appendices

The policies and the appendices 1 & 2 listed below can be found on our website.

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: Acceptable Use of ICT Policy - Students

Status	**Non Statutory**	**Date created**	**September 2021**
Any other statutory names for this policy (where applicable)		**Date first approved**	**December 2021**
Responsibility for this policy (job title)	**Deputy Headteacher**	**Date last reviewed**	Approved Spring 24
Governors' Committee with responsibility for its review	**Teaching & Learning**	**Frequency of review**	**Annual**
Tick here if Bucks Policy attached in its entirety		**To be put on the school website?**	**Yes**
Approval necessary	**Sub Committee**		

Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including senior leadership teams), governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for pupils
- Establish clear expectations for the way pupils engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

Breaches of this policy may be dealt with under our Behaviour Matrix.

AHS seeks to implement this policy through adherence to the procedures set out in this document, and through commitment to staff and pupil training.

This policy should be read in conjunction with other school policies on the Governance & Policy page of our website:

- Behaviour and Exclusions Policy including Behaviour Matrix and Anti-Bullying Strategy
- Data Protection and Confidentiality Policy
- Child Protection and Safeguarding Policy
- Equality Statement

By using computers at Aylesbury High School, you agree to abide by the following rules:

General Use

- You must not install programs or applications onto school devices, or bring software into school on external devices.
- You must not use school computers for commercial purposes (e.g. buying or selling goods).
- School computers must only be used for school-related activities and purposes.
- You may be liable to pay for damage caused to school owned devices by negligence or misuse.
- You must ensure passwords are kept confidential at all times. Passwords or accounts must not be shared with friends. If you suspect your account password has been compromised, please inform IT.
- You must abide by any rules or restrictions put in place for printing. All printing is monitored and printing privileges may be removed from students who abuse this facility.
- You must not attempt to alter or interfere with the configuration of school devices.
- You must not attempt to access, copy or alter the work and files of other students or members of staff.
- You must show consideration for others when using school computers and ensure that you do not harm, harass, offend or insult anyone.

Internet Use

- The internet must only be used for study purposes or school related activities.
- You must not use the internet to harm, harass, offend or insult anyone.
- You must not use the Internet to get, download, send, print or display any materials that are unlawful, obscene or abusive.

- You must respect the work and ownership of people outside the school, as well as other students and staff. This includes abiding by copyright laws.
- Use of chat rooms, forums and instant messaging apps is strictly prohibited in school.
- You must never share personal or sensitive information online, including: your full name, home address, telephone numbers, school name, pictures, photos or any other information that could be used to identify yourself or other students.
- You must be aware that all internet and email usage is monitored.

These are not exhaustive lists. The school reserves the right to amend these lists at any time. The Finance & Operations Director will use professional judgement to determine whether any act or behaviour not on the lists above are considered unacceptable use of the school's ICT facilities.

Exceptions 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. Applications for such exemption must be made in writing to the Headteacher.

Sanctions

By using computers at AHS, you realise and agree that access to the AHS computer network is a privilege, not a right and that this privilege may be revoked if these rules are broken. Additional action may be taken by the school in line with existing practice regarding inappropriate behaviour and if appropriate, the police may be involved or other legal action taken.

Pupils

Access to ICT facilities

The following ICT facilities are available to pupils, when instructed and supervised by the relevant member of staff:

- Computers and equipment in the school's ICT suites
- Specialist ICT equipment, such as that used for music, or design and technology

Pupils will be provided with an account linked to the school's Google Classroom, which they can access from any device, including their chromebooks, by using the following URL https://www.ahs.bucks.sch.uk/ .

- Student and staff passwords should be a minimum of eight characters, including numbers and letters, and all users should consider changing their password at regular intervals, perhaps once a term.
- One should not use one's own name or username as a password, for example smith1
- One should not use one's password on anything you leave unattended
- All users must change their password immediately if they think someone has learned their password
- All users must remember that a school is a public place. They must always make sure they have completely logged off or locked the computer before leaving it unattended. Failure to do so will be considered a contravention of school policy. If an offence has been committed by some other person on their unattended computer, this may be considered as facilitating the Misuse of a Computer, which is a criminal offence

Sixth-form pupils can use the computers in the ICT suites, library or sixth form centre independently for educational purposes only.

Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

Unacceptable use of ICT and the internet outside of school

- The school will sanction pupils, in line with the Behaviour & Exclusions Policy, if a pupil engages in any of the following at any time (even if they are not on school premises):
- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet 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
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- 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 ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Pupils who use the school's ICT facilities should use safe computing practices at all times.

Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Students who disclose account or password information may face disciplinary action.

Internet access
The school wireless internet connection is secured.

All students are given access to wifi whilst at school and this is in all areas of the school.

In Y7-11 we do this through the use of Chrome Education Upgrades which are added to each student's Chromebook. In Y12-13 our students are given codes for the BYOD network and can access wifi this way.

The Chrome Education Upgrade gives our IT team more control of what users access. It also allows for updates and apps to be pushed out to all users.

All students using the school wifi are subject to the Smoothwall filtering that the school subscribes to.

Additionally, we make use of Securly which allows teachers to see the screens of the students in their class and Smoothwall Monitoring and Filtering which alerts the DSL team to concerning activity from students.

Monitoring and review

The Finance & Operations Director and IT Manager will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year. The Teaching and Learning Committee of the Governing Board is responsible for approving this policy.

Appendix 2: Excerpts from the Staff Professional Behaviour Code

7. Acceptable use of Generative AI

Staff do not currently have access to generative AI resources on school devices and networks and all known generative AI resources are blocked; this is because we are not able to fulfil our safeguarding or GDPR obligations. We are aware that staff may well have access to such resources outside of school, we would remind staff that they should be extremely careful and ensure no AHS proprietary information is ever entered; any incidents of concern must be reported immediately. While there is no expectation for staff to be working from home outside of their working hours, we understand some staff may choose to. In such cases, where AI has been used, it is essential that materials are checked rigorously for accuracy, quality, data protection, alignment with school processes and policies and from a values perspective (values, norms and ethical aspects do not play a role in the creation of the text by AI). Any material created with the aid of AI is ultimately the teachers' responsibility.

Students do not have access to generative AI resources on School devices and networks and all known generative AI resources are blocked. This does not control students' personal devices or devices that are logged on to external internet sources such as 5G or hotspots. As such, it is essential that the use of devices is monitored by teachers in lessons, e.g. through the use of Impero, ensuring that device lids are closed when not in use, and issuing behaviour marks for inappropriate use of mobile phones. It is also important that staff circulate the room to monitor internet use, particularly for students in the Sixth Form who are not monitored by Impero. It is important that students are educated surrounding the safe, ethical and meaningful use of AI and this is addressed through L4L and Computing lessons and Current Issues for Sixth Form. For guidance surrounding setting and use of AI for homework tasks, see the Teaching and Learning Strategy.

The School has appropriate filters and monitoring in place to facilitate the safe use of non-generative AI technologies, however all staff members have a responsibility to ensure the security of any personal, sensitive or confidential information when using AI technologies. Staff should not input the names of students, staff, members of the school community, or any other sensitive information about students and staff into an AI tool. In the event of a data breach, it should be reported immediately in line with our Data Protection Policy. Accidental exposure to inappropriate material or unethical use of AI must be immediately reported to the DSL and will be logged. Depending on the seriousness of the offence, an investigation may need to be carried out.

11. Use of technology for online / virtual teaching

All staff should follow this guidance when conducting online/virtual teaching. They should display the same standards of dress and conduct that they would in the real world; they should also role model this to students and parents. The following points should be considered:-

- think about the background; photos, artwork, identifying features, mirrors – ideally the backing should be nondescript or the setting to blur the background should be applied.
- staff and students should be in living / communal areas – no bedrooms
- staff and students should be appropriately dressed
- filters at a child's home may be set at a threshold which is different to the school
- resources / videos must be age appropriate

It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and / or parent immediately and end the online interaction if necessary. Recording lessons on online meetings does not prevent abuse. If staff wish to record the lesson they are teaching, consideration should be given to data protection issues; e.g., whether parental / student consent is needed and retention / storage. If a staff member believes that a child or parent is recording the interaction, the lesson should be brought to an end or that child should be logged out immediately. Staff, parent and student AUPs clearly state the standards of conduct required.

23 c Staff IT Conduct

Staff guidance relating to their IT conduct is available both here, in the Staff Handbook and in the Staff Acceptable Use of IT Agreement. Staff will also be reminded of IT conduct related guidance via the Weekly Bulletin and through training organised by the School, at appropriate times.

Staff are also required to agree to the Staff Acceptable Use Agreement using a Google Form. The information gained from this process is monitored and reviewed by a member of the Senior Leadership Team.

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for students, staff (including the Senior Leadership Team), governors, volunteers and visitors. It supports the teaching and learning, and pastoral and administrative functions of the school. To support teaching and learning, if a member of staff requests access to a site that Smoothwall is blocking, the IT team will check a regularly updated document from Buckinghamshire Council, which lists sites that need to be blocked. The IT team also completes its own testing to ensure the site is safe; if the site links to social media or incorporates adverts access is not given.

e School email accounts and appropriate use

Staff should be aware of the following when using email in school:

- Staff should use their school email accounts for school-related matters, contact with other professionals for work purposes and to communicate with students, parents or carers. Personal email accounts should not be used to contact any of these people.
- For any awkward, sensitive, easily misinterpreted situations or anything that may have legal repercussions, staff should have the content of their email checked carefully by a member of the Senior Leadership Team.
- Staff must tell a member of the Senior Leadership Team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- Staff should refer to the Data Protection and Confidentiality Policy before sending any sensitive or personal data via email.
- We ask that staff consider the time of day that you are sending emails, especially avoiding times you wouldn't expect to use the phone. We would advise 0700 - 1900 on work-days and avoided at weekends, and ask that if staff are working at other times, emails are scheduled where possible/reasonable to protect staff wellbeing.

f Abuse of E-mail/Internet/other messaging and chat apps

The School will not accept any abuse of e-mail, internet or telephones. Such behaviour may result in disciplinary action.

Inappropriate use of the internet and email on school devices will result in disciplinary action. Examples include using the internet to access pornographic, racist or offensive material, or for personal financial gain, gambling, political purposes or advertising. Using email to harass, intimidate, humiliate or cause grievance will not be tolerated.

Staff should be aware that all internet data, browsing history and traffic on the school network is collected by the school's ISP and may be monitored by the school and third parties acting on behalf of the school.

Staff should be aware that all email content (be it present or historic), attachments and data are collected by Google Workspace and may be monitored and accessed by the school.

Staff are not permitted to use school email accounts for personal purposes. Staff should have non-school related, personal home accounts for non-school related internet and email usage.

Staff are not permitted to register or attach any school accounts to websites or internet services that are not related to school activities.

Staff are not permitted to subvert the school network and internet filtering systems. Usage of unauthorised third-party VPN applications is not permitted on school devices.

Staff should adhere to copyright regulations when downloading media onto a school computer, or device connected to the school network.

Staff are encouraged not to publish specific and detailed private thoughts on any social media sites, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff to remember that they are always representing the school and must act appropriately.

Safe and professional behaviour of staff online will be discussed at staff induction and guidance is provided both here and in the Staff Handbook.

Under the Obscene Publications Act 1959, an employee may have criminal liability if an individual publishes material that could corrupt or deprave the persons likely to see the material, this includes the transmission of data stored electronically.

Students will frequently set up social media groups (eg on WhatsApp for a trip or collaborative purposes). This is perfectly acceptable but staff should not join the group because of the privacy issues this would raise.

Appendix 3: Online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date:**
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	

ONLINE SAFETY TRAINING NEEDS AUDIT	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 4: Annual Review of online safety at AHS

Smoothwall Digital Safeguarding Checklist 2025

Appendix 5: Annual Risk Assessment

Online risk-assessment Feb 25