The Aylesbury Vale Academy Trust
The Aylesbury Vale Academy RESPECT | ASPIRATION | RESILIENCE

E- Safety Policy

Policy Reference:	163
Description:	This policy provides a framework for the Online Safety at Aylesbury Vale Academy.
Status:	Non statutory
Policy Audience:	Staff, Students & Parents/Carers
Academy Contact:	Academy Principal
Other related AVA policies and procedures:	Staff Grievance Policy, Gifts and Hospitality Policy, Child Protection
Governor Committee:	Governing Body
Approved by the Governing Board on:	12.10.2026
Latest Date for Next Review:	12.10.2027
Version + Schedule of Amendments:	V3
Signed:	
Date of Signature:	12.10.2026
In reviewing this policy, the Governing Board has had regard to the Equality Act 2010 and carried out an equality impact assessment. It is satisfied that no group with a protected characteristic will be unfairly disadvantaged by this policy.	

Contents

1. Aims....2
2. Legislation and guidance....3
3. Roles and responsibilities....3
4. Educating pupils about online safety....7
5. Educating parents/carers about online safety....9
6. Cyber-bullying....9
7. Acceptable use of the internet in school....9
8. Pupils using mobile devices in school....9
9. Staff using work devices outside school....9
10. How the school will respond to issues of misuse....10
11. Training....13
12. Monitoring arrangements....14
13. Links with other policies....12
Appendix 1 Student Internet Code of Practice....14
Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)....15
Appendix 3: online safety training needs – self audit for staff....16

1. Aims

The Aylesbury Vale Academy aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 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 or generating illegal, inappropriate or harmful content, including pornography, misinformation and disinformation, AI-generated content, 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, including the misuse of AI to create, alter or distribute harmful, abusive, sexualised or deceptive content.

- **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 2026 (KCSIE), and should be read alongside the Academy's Child Protection Policy.

This policy is based on the DfE's advice for schools on:

Keeping children safe in education 2026: September 2026

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

Relationships and sex education (RSE) and health education

Searching, screening and confiscation

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 Principal to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, staff newsletters and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking illegal, harmful and inappropriate content without unreasonably impacting teaching and learning, including, where technically possible and appropriate, harmful content in text, image, audio, video and AI-generated formats.
- Having effective monitoring strategies in place that meet their safeguarding needs.

The Academy will consider the safeguarding implications of AI-generated content when reviewing its filtering and monitoring provision.

All governors will:

- Ensure 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 Principal

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

3.3 The designated safeguarding leads

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

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

- Supporting the principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the principal and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- 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's child protection policy

- 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 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 principal and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy (PREVIOUSLY IN 3.4 THE NETWORK MANAGER)
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy (PREVIOUSLY IN 3.4 THE NETWORK MANAGER)
- Ensuring that safeguarding alerts or concerns arising from the Academy's monitoring systems are reviewed, triaged and, where appropriate, recorded on CPOMS and responded to in accordance with the Academy's Child Protection Policy.

This list is not intended to be exhaustive.

3.4 The Network manager

The Network manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually 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 a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites 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
- Ensuring that alerts generated by technical monitoring systems which may indicate a safeguarding concern are promptly shared with the DSL or safeguarding team in accordance with agreed escalation procedures.

- Working with senior leaders to support compliance with the DfE's current cyber-security standards, including cyber-risk assessment, account and access management, security updates, anti-malware and firewall protection, data backup arrangements and incident response.
- Immediately notifying the Principal, DSL and/or Data Protection Officer, as appropriate, where a cyber-security incident may present a safeguarding risk or involve the compromise of children's personal or safeguarding information.

This list is not intended to be exhaustive.

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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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 by reporting to the DSL using CPOMS immediately.
- Following the correct procedures by speaking with the Network Manager in advance if they need to bypass the filtering and monitoring systems for educational purposes
- 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/carers

Parents/carers 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 (appendices 1 and 2)

Parents/carers 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:

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- That online services and social media platforms have age restrictions and terms of use which pupils should understand and follow, and that these restrictions are intended to help protect children from inappropriate content, contact and other online risks.
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online

In **KS3**, 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 **KS4** 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:

- Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues
- The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online
- Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images
- That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Pupils should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Pupils should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Pupils should also understand that sharing indecent images of people over 18 without consent is a crime
- What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
- About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught where to go for advice and support about something they have seen online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong
- That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice
- How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns

- That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect pupils who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it
- How information and data is generated, collected, shared and used online
- That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
- That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion
- That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk

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/carers about online safety

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

Online safety will also be covered during parents' evenings.

The school will let parents/carers 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/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.

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

6. Cyber-bullying

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 cyber-bullying

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. Teachers will discuss cyber-bullying with their tutor groups.

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/carers so 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 Principal, and any member of staff authorised to do so by the Principal, 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 Principal and/or the DSL
- 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 co-operation

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 DSL, Principal or 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/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image or video 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.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are increasingly available to staff and pupils. The Academy recognises that generative AI can provide educational benefits but can also introduce safeguarding, data protection, privacy, security and educational risks.

These risks may include exposure to or generation of harmful or inappropriate content, inaccurate or misleading information, bias, impersonation, manipulation, deepfakes, cyber-bullying, the sharing or creation of sexualised material, inappropriate emotional reliance on AI systems, and the disclosure of personal or sensitive information.

The Academy will consider the safeguarding implications of generative AI when introducing or approving AI products for use by staff or pupils. Appropriate consideration will be given to the product's intended age group, filtering and monitoring arrangements, privacy and data protection, security, accessibility and the needs of vulnerable pupils and pupils with SEND.

Staff and pupils must not enter confidential, safeguarding, special category or other sensitive personal information into generative AI systems unless the Academy has specifically approved the system and its use for that purpose.

The creation, alteration or distribution of AI-generated content for the purpose of bullying, harassment, sexual harassment, abuse, impersonation or humiliation will be dealt with in accordance with the Academy's Behaviour Policy, Child Protection Policy and, where appropriate, reported to external agencies.

Where the Academy introduces AI products for pupil use, consideration will be given to the DfE's Generative AI Product Safety Standards and relevant data protection requirements.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school in their school bag but are not permitted to use them whilst on the school site.

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:

- Using secure passwords/passphrases in accordance with the Academy's current cyber-security requirements and never sharing passwords or authentication credentials with others.
- Ensuring their hard drive is 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
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates
- Using multi-factor authentication where required by the Academy.

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must not upload personal data, special category data, confidential Academy information, safeguarding records or identifiable pupil work to an externally hosted AI system unless its use has been approved by the Academy and complies with the Academy's data protection arrangements. Where the proposed use presents a high risk to individuals' rights and freedoms, the Academy will consider whether a Data Protection Impact Assessment is required before implementation.

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 Network 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 behaviour policy. 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 code of conduct and disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11.1 Staff

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, staff 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
- Generative AI presents emerging safeguarding risks, including harmful or inappropriate generated content, misinformation and bias, deepfakes and impersonation, privacy and data protection concerns, and the potential for AI systems to facilitate bullying, harassment or abuse.

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 DSLs 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 policy.

11.2 Pupils

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

12. Monitoring arrangements

The DSL logs safeguarding issues related to online safety using CPOMS.

The Academy will formally review its filtering and monitoring provision at least annually, and following any significant safeguarding incident, technological change or change of provider where appropriate. The review will involve the DSL, senior leadership, Network Manager/IT support and appropriate representation from the governing board.

The review will consider whether the Academy's filtering and monitoring provision continues to meet its safeguarding needs, including the needs of vulnerable pupils and pupils with SEND, emerging technologies and risks associated with AI-generated content.

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

13. Links with other policies

This online safety policy is linked to our:

- Child protection policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1 Student Internet Code of Practice

1.1 STUDENT INTERNET CODE OF PRACTICE

Access to the school internet system will only be permitted once the following has been read and signed by both yourself and your child. The Academy reserves the right to administer these rules in a fair and unbiased way, which may result in a child's access either to the Internet or the school network being removed or other appropriate sanction being taken. The code of practice follows:

- I will only use the internet when supervised by a teacher or an appropriate adult.
- I will never tell anyone I meet on the internet my home address, my telephone number or my school's name, unless my teacher specifically gives me permission.
- I will never send anyone my picture without permission from my teacher/parent/carer.
- I will never give my password to anyone; even my best friend and I will log off when I have finished using the computer.
- I will never arrange to meet anyone in person without first agreeing it with my parents/carer/teacher and get them to come along to the first meeting.
- I will never access an online chat-room without permission from my teacher/carer/parents.
- I will never respond to unpleasant, suggestive or bullying e-mails or bulletin boards and I will always report it to a teacher or parent/carer.
- I will not look for bad language or distasteful images while I'm online and I will report bad language or distasteful images to a teacher or parent/carer if I come across them accidentally.
- I will always be myself and will not pretend to be anyone or anything I am not.
- I will not take information from the internet and pass it off as my own work.
- I am aware that my teacher, ICT staff and the Academy's Internet Service Provider will check the sites I have visited.
- I understand that I can only access material relevant to my school work and must not deliberately look at unsuitable material.
- I will not deliberately attempt to set-up or use any proxy by-pass software in order to by-pass the school internet filter.
- I know that the posting of anonymous messages and the forwarding of chain messages is not allowed.
- I know that the contents of my e-mail messages will be monitored by relevant staff and software.
- I will not download software from the Internet, including screen savers, games, video clips, audio clips, *.exe files.
- I will not play online games as this takes up network resources and may introduce harmful viruses to the network.
- I know that information on the Internet may not always be reliable and sources may need checking. Websites may be sponsored by advertisers.
- I will not use e-mail to send or encourage material which is pornographic, illegal, offensive or annoying or invades another person's privacy.

I understand and agree to adhere to the Student Internet Code of at Aylesbury Vale Academy.

Student Signature _____ Date: .....

Parent/Carer Signature: ..... Date: _____

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

All staff (including supply and temporary) requiring Internet access should sign a copy of this Acceptable Use Statement and return it to the IT Team/HR
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will abide by the below:

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Governing Body.
- I will not use my school email address to access social media networks or chat rooms.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal or Governing Body.
- I will not connect any unauthorised hardware or devices to the school's equipment.
- I will not attempt to install unauthorised software without permission of the Principal.
- I will not share confidential information about the school, its pupils or staff, or other members of the community.
- I will only open email attachments from sources I know to be safe.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will NOT give my ID card / Keys to students at ANY time.
- Images of pupils and / or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Principal.
- Personal devices will not be used to take images of anyone.
- I understand that all my use of the Internet and other related technologies can be monitored, logged and made available, on request, to the Principal.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will respect copyright and intellectual property rights of service providers. I will not 'rip content' from the likes of YouTube using school owned equipment and attempt to store it on the school's network.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will be responsible for content I put onto the Academy's network / cloud storage and delete it when no longer needed.
- I will support and promote the school's E-Safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- Access to the internet and school server should only be made via the authorised account and password, which should not be made available to any other person.
- It is the responsibility of staff members to make the IT Team aware of occasions when passwords cease to become private.
- Staff should ensure that high levels of data-protection are adhered to at all times. This means locking classroom doors and computers whilst leaving the room.
- Issued Academy owned equipment are for staff use only, not family members. These devices will be

encrypted.

- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- Permission should be granted from the Principal before bringing in electrical and ICT equipment from home.
- Users are responsible for all emails sent and for contacts made that may result in email being received.
- Use of Academy equipment for personal financial gain, gambling, political purposes, online shopping or advertising is forbidden.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As email can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- No reference should EVER be made to The Aylesbury Vale Academy on any social networking site.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- I understand this forms part of the terms and conditions set out in my contract of employment.
- I will immediately report any suspected personal data breach, loss of information or cyber-security incident in accordance with the Academy's Data Protection and Cyber-Security procedures. Where the incident involves safeguarding information or may place a child at risk, I will also immediately inform the DSL.

When using generative artificial intelligence (AI) tools in connection with my role, I will:

- Only use AI tools and services approved by the Academy for the intended purpose.
- Follow Academy policies and guidance relating to AI, data protection, safeguarding, confidentiality and acceptable use.
- Never enter confidential information, safeguarding information, special category data, CPOMS records or identifiable sensitive information about pupils, families or staff into an AI system unless the Academy has expressly approved the system and its use for that purpose.
- Check AI-generated information for accuracy, appropriateness, bias and suitability before using or sharing it.
- Remain professionally responsible for any material that I produce or communicate with the assistance of AI.
- Never use AI to create, manipulate or distribute harmful, abusive, discriminatory, sexualised, deceptive or inappropriate content, including deepfake images, audio or video.
- Immediately report any AI-generated content or use of AI which raises a safeguarding concern in accordance with the Academy's safeguarding procedures.
- Follow Academy expectations relating to copyright and intellectual property when using AI-generated content.

User Signature

- I agree to follow this code of conduct and to support the safe use of ICT throughout the school Any breaches in the operation of the requirements laid out in this Acceptable Use Statement will result in the Disciplinary Policy being invoked.

Signed (staff member/governor/volunteer/visitor):	**Date:**

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?	
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?	