



Alder Community
High School

Online Safety Policy

Author:	Keith Doran / Rachel Anderson		
This policy was agreed by Governing Body. This policy supersedes all previous policies relating to this area.			
Implemented:	Spring 2026	Review date:	Spring 2027
Statutory Required to be on school website			

Contents

1. Aims	2
2. Legislation and guidance	3
3. Roles and responsibilities	3

4. Educating pupils about online safety	6
5. Educating parents/carers about online safety	7
6. Cyber-bullying.....	8
7. Acceptable use of the internet in school.....	10
8. Pupils using mobile devices in school.....	10
9. Staff using work devices outside school.....	10
10. How the school will respond to issues of misuse.....	11
11. Training for staff, governors and volunteers.....	11
12. Monitoring arrangements	11
13. Links with other policies	12

1. Aims

Our school aims to:

- › Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors, visitors and contractors.
- › 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 illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, 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 the user 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](#)

- › [Meeting digital and technology standards https://www.gov.uk/government/publications/preventing-and-tackling-bullying](https://www.gov.uk/government/publications/preventing-and-tackling-bullying)
- › [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 headteacher to account for its implementation and effective functioning.

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, e-bulletins 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 and requirements for training.

The Governing Board will ensure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that 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's filtering and monitoring standards](#), and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- › Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- › Reviewing filtering and monitoring provisions at least annually
- › Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- › Having effective monitoring strategies in place that meet the school's safeguarding needs

The Governing Body will designate a link Governor who will have responsibility for overseeing and monitoring this policy.

All Governors will:

- › Make sure they have read and understand this policy
- › Agree and adhere to the terms on acceptable use of the school's ICT systems, the school network and the internet.
- › Make sure that online safety is a running and interrelated theme when devising and implementing the whole school approach to safeguarding and related policies and/or procedures

- › Make sure 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 be more suitable

3.2 The Headteacher

The Headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead (DSL)

Details of the school's Designated Safeguarding Lead (DSL) and Deputy 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 making sure that staff understand this policy and that it is being implemented consistently throughout the school
- › Working with the Headteacher and Governing Board to review this policy annually and make sure 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
- › Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- › Working with the ICT Network Manager to make sure the appropriate systems and processes are in place
- › Working with the Headteacher, ICT Network 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
- › Responding to safeguarding concerns identified by filtering and monitoring
- › Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- › Making sure 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 headteacher and/or governing board
- › Undertaking annual risk assessments that consider and reflect the risks pupils 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

This list is not intended to be exhaustive.

3.4 The ICT Network Manager

The ICT 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 make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- › Making sure 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 monthly basis
- › Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- › Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- › Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All Staff and Volunteers

All staff, including visitors, 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, and making sure that pupils follow the school's terms on acceptable use
- › 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 contacting the DSL or Deputy.
- › Following the correct procedures by contacting the DSL or Deputy if they need to bypass the filtering and monitoring systems for educational purposes
- › Working with the DSL to make sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- › Making sure 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
- › Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

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](#)
- › Help and advice for parents/carers – [Childnet](#)
- › Parents and carers resource sheet – [Childnet](#)

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 and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Educating Pupils about Online Safety

4.1 Pupils will be taught about Online Safety as part of the Curriculum

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:

- › The power and richness of online resources, and how to use them effectively
- › 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.

4.2 Pupils will be taught Practical Cyber Security Skills

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 education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

5. Educating Parents/Carers about Online Safety

The school will raise parents/carers' awareness of internet safety in newsletters or other communications home, and in information via our website and our online safety hub. 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 Headteacher and/or the DSL.

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

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 encourage them 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 classes.

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

- › Poses a risk to staff, pupils, or others 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

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 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 whether 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 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 AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Alder Community High School recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Alder Community High School will treat any use of AI to bully pupils very seriously, in line with our anti-bullying policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

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). 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 agreement.

8. Pupils using Mobile Devices in School

Pupils may bring mobile devices into school but are not permitted to use them anywhere on the school site at any time (including before and after the school day). Mobile devices should be switched off at the gate and placed in the students' bag or locker.

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 devices are password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager. Staff laptops automatically lock if left inactive for a period of time. Storage on laptops is encrypted - this means if the device is lost or stolen, no one can access the files stored on them. Antimalware software and operating systems are updated promptly with the latest updates.

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

- › All additional secondary storage devices (e.g. memory sticks) 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.
- › Not sharing the device among family or friends

Staff members must not use the device in any way that 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 ICT 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 policies on 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. 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. Training for Staff, Governors and Volunteers

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, threatening, 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 Deputy 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 logs of behaviour and safeguarding issues related to online safety are logged on CPOMS.

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 and safeguarding policy
- > Behaviour policy
- > Staff disciplinary procedures
- > Data protection policy and privacy notices
- > Complaints procedure

> ICT and internet acceptable use policy