ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

Online Safety Policy

This is part of a suite of policies for safeguarding children. Please also see our Child Protection and Safeguarding Policy for more.

Approved by: David Preston, Headteacher & Director
Di Gardiner, Safeguarding Director
Laura Sweetman, DSL & Head of School
Wynford Dore, Chair of the Board
Gareth Newman, Proprietor & Director
Rosie Sayers, Director
Geraint Newman, Director
Sanj Dhadda, Commercial Director

Date: 17.11.25

Last Reviewed: 17th November 2025

Review Period Annually

Next Review Due: 1st September 2026

Contents

1. Aims

Our school aims to have a robust whole school approach to online safety, ensuring that it is a running and interrelated theme within our safeguarding provision and practice. At ALS, we aim 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')
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Ensure high quality training for online safety that creates an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk, which we know to be considerable and ever-evolving:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism, misinformation, disinformation (including fake news) and conspiracy theories
- **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 scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) 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 (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.

This policy also reflects the DfE's Cyber Security Standards for Schools and Colleges and guidance from the National Cyber Security Centre (NCSC). The school commits to:

- Meeting the cybersecurity standards to improve resilience against cyber-attacks
- Reviewing cybersecurity measures regularly with governors and IT staff
- Implementing appropriate technical and organisational measures to protect school systems and data
- Providing cyber security awareness training for all staff

3. Roles and responsibilities

3.1 The Board of Directors

The Board of Directors has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The Headteacher, on behalf of the Board of Directors, will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Director who oversees online safety is the Safeguarding Director, outlined in the Child Protection & Safeguarding Policy.

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

The Directors will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The Directors 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

All Directors 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 SEND 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 DSL and DDSLs are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL holds the role of Online Safety Lead at Arnold Lodge School. Where the DSL delegates specific online safety responsibilities, this will be documented and the overall accountability remains with the DSL. The Online Safety Lead is responsible for ensuring a whole-school approach to online safety that integrates with the broader safeguarding framework.

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 consistently throughout the school
- Working with the headteacher 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
- Providing the Board of Directors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- 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
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged (see appendix 5) 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 (appendix 4 contains a self-audit for staff on online safety training needs)
- 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 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

This list is not intended to be exhaustive.

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 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 fortnightly 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 (see appendix 5) 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

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)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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 (appendices 1 and 2)

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
- Healthy relationships – Disrespect Nobody

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 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 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

By the **end of Juniors**, pupils will know:

> That people sometimes behave differently online, including by pretending to be someone they are not

> That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous

> The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

> How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

> How information and data is shared and used online

> What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

> How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

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:

- 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.

Harmful Online Challenges and Hoaxes:

The school educates pupils about harmful online challenges and online hoaxes as part of the online safety curriculum. Pupils are taught to:

- Recognise when online challenges may pose risks to their safety or wellbeing
- Understand that viral trends and challenges can be dangerous even if they appear popular
- Question the authenticity of online content and identify potential hoaxes
- Report concerns about harmful challenges to a trusted adult immediately
- Support peers who may be pressured to participate in risky online activities

The school monitors emerging online trends and challenges that may affect pupils and provides timely information to staff and parents when specific risks are identified. Parents are encouraged to discuss online challenges and trends with their children and to contact the school if they have concerns. Resources on harmful online challenges are available at: https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes

External Visitors and Online Safety Education:

Where the school engages external visitors to deliver online safety education to pupils, parents, or staff, the school follows UKCIS External Visitors Guidance to ensure maximum impact and safeguarding. This includes:

- Vetting external providers and ensuring they have appropriate safeguarding training and DBS checks
- Reviewing session content in advance to ensure age-appropriateness and alignment with school values
- Ensuring a member of school staff is always present during sessions
- Integrating external input into the school's broader online safety curriculum
- Evaluating the impact of external sessions and gathering feedback from participants

The school prioritises evidence-based approaches to online safety education and selects external providers accordingly.

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.

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. 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 one 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. Please see out Anti-bullying Policy for more detail.

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. Class teacher & mentors will discuss cyber-bullying with their mentor 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 education(PSHEE), and other subjects where appropriate.

All staff, appropriate Directors 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).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Policy and Anti-Bullying 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 consider whether the incident should be reported to the police if it involves illegal material, and will 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 DSL.
- Explain to the pupil why they are being searched, and 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 the staff member in conjunction with the DSL 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

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.

ALS 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.

ALS will treat any use of AI to bully pupils very seriously, in line with our anti-bullying & behaviour 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 by the school/trust, 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.

Arnold Lodge School recognises the educational potential of generative AI tools while being mindful of safety considerations. The school follows the DfE's "Generative AI: product safety expectations" guidance and ensures that:

- Filtering and monitoring requirements apply to the use of generative AI tools in education
- Staff assess age-appropriateness before introducing AI tools to pupils
- Pupils are taught critical thinking skills to evaluate AI-generated content
- Privacy implications are considered when using AI tools that may process personal data
- Staff understand that AI tools should supplement, not replace, teacher expertise and judgment

Any use of generative AI tools will be in accordance with the school's AI Usage Policy and data protection requirements. Staff should be aware that AI-generated content may contain inaccuracies, biases, or inappropriate material, and should review AI outputs before sharing with pupils.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and Directors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). 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.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school if they are required for contacting parents on the journey to and from school and mobile phones are not permitted to be turned on or use at any reason at any point during the school day. In part, the

full ban on mobile phones is down to the fact that we recognise that pupils will potentially have unlimited and unrestricted access to the internet via mobile phone networks and these may be used in a negative way by pupils towards their peers.

Please see the Pupil Information Booklet on the Pupil Portal for more information.

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)
- 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 – always install the latest updates

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

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, Acceptable use of ICT and Online Safety. 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, Handbook and Planner. 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, online training courses 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 other children 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 the risks up
- 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 DDSLs 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.

Directors, particularly the Safeguarding Director, 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.

11a. Information Security and Access Management

The school recognises its direct responsibility to ensure appropriate security protection procedures are in place to safeguard systems, staff, and pupils. These procedures are reviewed periodically to keep pace with evolving cybercrime technologies.

Information security measures include:

Technical Controls:

- Multi-factor authentication for staff accessing school systems remotely
- Regular software updates and patch management
- Secure password policies (minimum 8 characters, complexity requirements, regular changes)
- Network segmentation to protect sensitive data
- Regular backups of critical data with tested recovery procedures
- Encrypted storage for sensitive pupil and staff information

Access Management:

- Role-based access controls ensuring staff only access data necessary for their role
- Regular review of user access permissions, particularly when staff change roles or leave
- Guest network provision for visitors, separate from the main school network
- Secure procedures for managing privileged administrator accounts

Incident Response:

- Documented procedures for responding to suspected data breaches or cybersecurity incidents
- Requirement to report security incidents immediately to the IT Manager and DSL
- Regular testing of incident response procedures

Governance:

- The Board of Directors receives regular updates on cybersecurity risks and measures
- Annual review of cyber security arrangements against NCSC and DfE standards
- Cybersecurity is considered part of the school's overall risk management framework

Further guidance is available from:

- National Education Network e-security guidance
- National Cyber Security Centre (NCSC): https://www.ncsc.gov.uk/
- DfE Cyber Security Standards for Schools and Colleges

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. This is primarily through MyConcern and the Incident and Bullying Log for that academic year.

This policy will be reviewed every year by the DSL. The updated policy will be shared with the Board of Directors at the first board meeting of each new academic year. The updated policy will be supported by the live ALS online safety self-review tool produced by South West Grid for Learning (SWGfL), an example of which can be found here.

This review tool forms the basis of the half termly meetings between the DSL and the school's Online Safety Coordinator, and is used to reflect on the risks pupils face online and how we as a school are doing everything we can to mitigate those risks and educate our pupils in staying safe online. This live self-review tool is important because technology, and the risks and harms related to it, evolve and change rapidly.

The annual review will be supported by a comprehensive online safety risk assessment that:

- Considers and reflects the current and evolving risks that pupils face online
- Evaluates the effectiveness of the school's filtering and monitoring systems
- Assesses the impact of online safety education across all year groups
- Identifies emerging technologies, platforms, and online risks relevant to the school community
- Reviews incident logs and trends to inform policy updates

The policy will be reviewed sooner if there are legislative updates, significant safeguarding incidents, or changes at the school that impact online safety provision.

13. Remote Education

At ALS, pupils are entitled to remote learning in the following circumstances:

- The school is closed to pupils during term time
- A pupil has COVID-19
- A pupil is unable to attend school due to other extenuating circumstances (this arrangement is agreed on a case by case basis between the parents/guardians and the head of school).

In these circumstances, ALS recognise our responsibility to keep our pupils safe online and follow the advice pages hyperlinked in Keeping Children Safe in Education (2022) in our guidance for staff, which they are issued as a remote learning agreement:

Safeguarding and remote education - GOV.UK (www.gov.uk)
Undertaking remote teaching safely | NSPCC Learning

Pupils are also provided with a remote learning agreement which they are asked to read before commencing remote learning for any period of time. This agreement primarily focuses on acceptable behaviours whilst working remotely and staying safe online. The remote learning agreements for staff and pupils are available on request.

At ALS we recognise that during periods of remote learning it is our responsibility to stay in regular contact with parents and carers, to reinforce the importance of ensuring that their child is staying safe online and what their child is being asked to do.

14. 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

Appendix 1: EYFS and KS1 and 2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends.
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS3-5 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

All pupils in Years 7-13 are expected to bring in a laptop or Microsoft Office compatible tablet (Bring Your Own Device) to allow them to complete and store work electronically. Devices remain the responsibility of the pupil whilst in school, and care should be taken to ensure that they are stored securely and protected from damage. All pupils are required to read and sign the following ICT acceptable use policy before using their own device in school or school ICT equipment.

I agree to keep my personal information safe.
Do not give out personal information like email addresses, home or school addresses or phone numbers to people you do not know. Do not share your passwords and log in details. Only post photos that you would be happy with your parents seeing. Once a photograph is online, you can ***never*** *stop it being sent to others.*

I agree to only access sites that are appropriate for my age and to download appropriate content and I will tell adults about any sites that I am worried about.
You must not attempt to access sites that contain inappropriate ***and illegal*** *content or sites that distract you from your learning. You must not attempt to get around any security systems in school. If something you need for work is blocked, you can request the site to be unblocked by the IT department.*

I agree to report my worries I have to an adult.
If a message makes you worried or uncomfortable tell an adult, such as a teacher or family member or friend. You can also click on the 'Report abuse' button on websites and Apps. If you receive an upsetting message or you feel bullied online, ***keep a copy*** *of the message and show it to an adult you trust.*

I agree to only send appropriate content via internet, SMS or MMS.
Never send any documents that are in any way inappropriate, offensive or illegal. Taking or sharing photos or videos in School is not permitted.

I agree not to use digital technology to write hurtful comments, bully or make threats.
Always respect others - cyberbullying is not acceptable. Treat people as you would like to be treated.

I agree to follow all ICT classroom school rules.
This includes protecting the ICT equipment from spillages by not eating or drinking near computers. You should take care of all ICT equipment and report any instances of vandalism to a member of staff.

My teachers and parents can provide me with guidance and support to help protect myself from potential danger and harm while using ICT. However, I am responsible for my actions and it is my responsibility to keep myself and others safe online and while using other technologies. I understand that the school must take appropriate action if I have broken the ICT Acceptable Use Policy. I understand that this may mean restricting my access to the school ICT systems.

Signed: _____**(parent/guardian on behalf of pupil)**
Print name: _____ **Date:** _____

Appendix 3: 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:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: 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?	