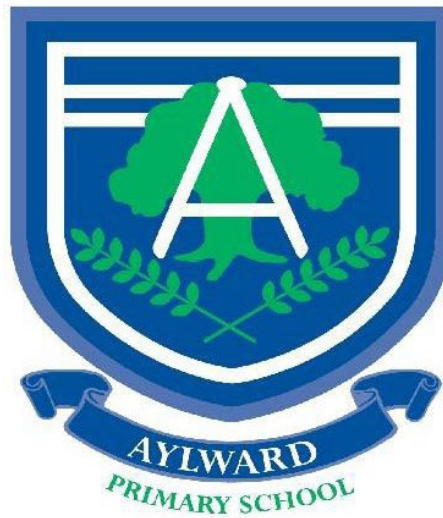




AYLWARD PRIMARY SCHOOL

Online Safety Policy

GB Committee Responsible:	Curriculum and Achievement
Reviewed by:	Emma Carey
Review Date:	September 2026
Approved by Committee:	24 th September 2026
Next Review Date:	September 2027

The purpose and scope of the policy

- To educate pupils about online safety issues and appropriate behaviours so that their actions remain safe and legal online.
- To help pupils develop critical thinking skills to reflect and enable them to keep themselves safe.
- To keep any personal data and information secure.
- To minimise the risks of handling sensitive information.

This policy should be read in conjunction with the following school policies, which are available on the school's website:

- Safeguarding and child protection policy
- Anti-bullying policy
- Behaviour policy
- Data protection policy
- Relationship and health education policy
- Allegations against staff policy.

Different Technologies

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently, the internet technologies children and young people are using both inside and outside of the classroom include (but are not exclusive to):

- Websites
- Learning Platforms (SharePoint) and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Downloading from the internet
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality
- Accessing AI platforms/ tools within apps or programmes

At Aylward Primary School, we understand the responsibility to educate our pupils in online safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Risks

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate. All staff have a responsibility to safeguard pupils and recognise that safeguarding includes preventing online harms.

It is important to be aware that incidents occurring online or outside of school may still have a significant safeguarding impact on pupils or staff within the school.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk. The 4C's underpin the basis of our Online Safety Policy. They are:

- **content:** being exposed to illegal, inappropriate or harmful material or attitudes (e.g. racism/ extremism/ misogyny) and being exposed to misinformation/ disinformation (including fake news) and conspiracy theories. This also includes content that is AI-generated.

- **contact:** being subjected to harmful online interaction with other users, including generative AI applications that simulated human interactions
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm including – online bullying; making, sending or receiving explicit images; AI-generated explicit images
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Roles and Responsibilities

As online safety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named online safety leaders in our school are Emma Carey and Tiana Moore. All members of the school community have been made aware of who holds this post. It is the role of the online safety leader/s to keep abreast of current issues and guidance through organisations such as CEOP and 'Think U Know'.

The online safety leader/s update Senior Leadership Team and Governors. All Governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Writing and reviewing the Online Safety policy

This policy (for staff, governors, visitors and pupils), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: ICT, Home -school agreements, Behaviour, Health and Safety, Child Protection, and PSHCE policies including Anti-bullying.

Our Online Safety policy has been agreed by the Senior Leadership Team and Staff. The Online Safety policy and its implementation are reviewed annually.

Online Safety skills development for staff

- All members of staff receive regular information and training on online safety issues through the leader/s at relevant staff meetings and when appropriate in the school newsletter.
- Time is set aside in the first term of each academic year for an Online Safety update to all staff.
- All members of staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.
- All new members of staff receive information on the school's Acceptable Use Agreement as part of their induction.
- All members of staff incorporate online safety activities and awareness throughout children's learning.

Community use of the Internet

- External organisations using the school's ICT facilities must adhere to the online safety policy.

Teaching and Learning

- The school provides opportunities within a range of curriculum areas to teach online safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the online safety curriculum.
- Pupils are made aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, learning mentors, school counsellor or an organisation such as Childline/CEOP.
- Pupils are taught how to use technology safely, respectfully and responsibly, discuss the consequences of inappropriate online behaviour and know to report inappropriate behaviour to trusted adults.
- Pupils are educated in the effective and safe use of the Internet in research, including the skills of knowledge location, retrieval and evaluation to develop their critical thinking skills.
- Pupils are educated in the safe and appropriate use of AI technologies, in a manner that is appropriate to their age and stage of learning. They are taught how to use AI safely and responsibly, including how to protect their personal information, and to apply critical thinking

skills to make informed judgements about the accuracy, reliability and suitability of AI-generated information and content.

Managing Internet Access

- Anti-Virus protection and system security is updated and overseen by our IT technicians (AIT)

E-mail

- Pupils may only use email accounts linked to SharePoint on the school system.
- Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission.

Published content and the school web site

- The contact details on the school website are the school address, email and telephone number.
- Staff or pupils' personal information is not published in line with GDPR.
- The head teacher takes overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Written permission from parents or carers is obtained before photographs of pupils are published on the school website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Where possible, pupils' full names will not be used in association with photographs anywhere on the school website.
- Pupils' work can only be published by outside agencies with the permission of the pupil and parents.

Photographs taken by parents/carers for personal use

In the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites, e.g. school performances and assemblies etc.

Social networking and personal publishing

- The school blocks access to social networking sites for pupils.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate and or illegal (e.g. Facebook) for primary aged pupils.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff are advised not to add children, or parents as 'friends' if they use these sites.

Use of artificial intelligence (AI)

- Artificial intelligence (AI) refers to technologies that can perform tasks which would ordinarily require human intelligence. Generative AI is a type of AI that can create new content, including text, images, audio, video and code, in response to prompts.
- AI may be used by staff as a support tool for appropriate purposes – including lesson planning, resource creation, feedback and administrative tasks. Staff remain responsible for checking the accuracy, appropriateness, quality and suitability of any content produced using AI before it is used or shared.
- The use of AI as a teaching and learning tool must be carefully considered, risk assessed and appropriately controlled. Any AI tools used with pupils must be approved by the school and be appropriate for the relevant age and stage of learning. The school will comply with any age restrictions and terms of use that apply to AI tools.
- Pupils will only use generative AI where this has been specifically authorised by the school and under the supervision of a member of staff. The school will determine which AI tools, if any, are appropriate for use by pupils and for which year groups or learning activities. Pupils must not independently access or use unapproved AI tools in school.
- Where pupil-facing AI is used, appropriate safeguards will be in place, including suitable

supervision and, where applicable, appropriate safety, filtering and monitoring arrangements.

- The school will consider safeguarding, data protection, privacy, intellectual property, educational and ethical implications when selecting and using AI tools. AI tools must comply with applicable data protection laws, including the UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025.
- Staff and pupils must not enter personal, sensitive or confidential information about themselves or others into AI tools unless this has been specifically authorised and appropriate data protection arrangements are in place.
- Pupils are taught, in an age-appropriate way, that AI generated content may be inaccurate, unreliable, biased, misleading, inappropriate or unsafe and that AI can produce convincing information that is fake or taken out of context. Pupils are taught to apply critical thinking skills to check information against reliable sources before accepting or sharing it.
- Pupils are taught to use AI respectfully, safely and responsibly and to understand that AI-generated content can have consequences for themselves and others. This includes age appropriate awareness of misinformation, harmful content and online manipulation, including the risks associated with AI applications that simulate human interaction.
- Pupils are taught that AI can be used to create or manipulate images, audio and video, including deepfakes at an appropriate level to their age and stage of learning. The creation, possession or sharing of harmful, abusive or sexualised AI-generated images involving children is a safeguarding concern and will be dealt with in accordance with the school's safeguarding and child protection procedures.
- Any concerns arising from the misuse of AI tools, including bullying, harassment, grooming, exploitation, harmful or inappropriate content, the creation or sharing of explicit or inappropriate images, or AI-generated/ deepfake images must be reported in accordance with the school's safeguarding procedures.
- The school will keep its use of AI under review as technology and associated risks develop. AI use will be considered as part of the school's wider online-safety risk assessment and policy review.

Use of personal mobile devices (including phones)

- The Headteacher authorises the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.

- Pupils are not permitted to access the school's Wi-Fi system at any time using their mobile devices and hand-held computers.
- Mobile devices are not permitted to be used during school hours by pupils. Mobile phones owned by pupils are handed in to the school office at the beginning of the day and then collected at the end of each day. Parents need to seek written permission for their child to bring their mobile phone to school. This is limited to just Years 5 and 6 pupils.
- Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- Personal mobile devices will not be used to take images or videos of pupils or staff.
- Where permission has been granted, the school is not responsible for the loss, damage or theft on school premises of any personal mobile device.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

- The school will be especially alert to instances of online bullying and will treat such instances as a matter of high priority.

Use of webcams

- Pupils are not permitted to use webcams in school without permission from a member of staff.
- When using a webcam in school, pupils must do so with a member of staff present.
- Staff must consider whether it is appropriate to use a webcam as part of a learning activity. Where used, staff must be sensitive to pupils for whom it is inadvisable to appear online. (e.g. those without parental permission for photos to be published online, children for whom there are child protection concerns)

Filtering and Monitoring

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. The school currently uses London Grid for Learning (LGFL) as the filtering platform.
- Effective filtering systems are established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.
- Filtering systems used are relevant to pupils' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.
- The governing body ensure that use of appropriate filters and monitoring systems does not lead to 'over blocking', such that there are unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
- The school uses Securus to monitor Internet usage. The Headteacher receives a weekly report of usage, which is reviewed accordingly.
- Alongside the use of the filtering and monitoring system, staff have a responsibility to report and record any inappropriate content/ searches, or access issues to the Headteacher.

Protecting personal data

The school uses information about pupils to further curriculum, professional and managerial activities in accordance with the data protection policy and retention of documents policy.

Policy Decisions

Authorising Internet access

- Pupil instruction in responsible and safe use will precede any Internet access and all pupils must sign up to the Acceptable Use Agreement for pupils and abide by the school's online safety guidelines. Parents sign on behalf of children when they start school.
- Access to the Internet will be directly supervised and to specific, approved on-line materials.
- All staff using a school laptop will be made aware of the schools Laptop Use Policy.

Password Security

- Adult users are provided with an individual network username and password, Sharepoint username and password, which they are encouraged to change periodically.
- Pupils are provided with a Sharepoint username and password.
- All members of staff are aware of the dangers inherent in leaving the Arbor system, for pupil-tracking and digital registers, open and of the importance of keeping passwords secret.
- All members of staff are aware of their individual responsibilities to protect the security and confidentiality of the school network.

Handling online safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff and reported to the online safety leader(s) and recorded on CPOMS.
- Deliberate access to inappropriate materials by any user will be reported to the online

safety leads & senior leadership team and lead to the incident being logged by the online safety leaders.

- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints and concerns of a child protection nature must be dealt with in accordance with school child protection procedures. For example, evidence of: inappropriate online relationships; a child watching pornography or any '18' films on a regular basis; online/digital bullying, harassment or inappropriate image sharing etc.

Introducing the online safety policy to pupils

- Online safety rules are discussed with the pupils at the start of each term.
- Pupils are informed that network and Internet use will be monitored.
- The school is vigilant when conducting 'raw' image search with pupils e.g. Google search
- Pupils' parents are required to individually sign an online safety / acceptable use agreement form which is fully explained and used as part of the teaching programme.
- Posters of our acceptable use policy are on display in classrooms and children are reminded of the expectations when online at the beginning of each year.
- Our school is committed to ensure that children with disabilities or special educational needs have exactly the same human rights to be safe from abuse and neglect, to be protected from harm and achieve the same outcomes as non-disabled children. We recognise that disabled children or those with special educational needs may require additional action to ensure they have an understanding of online safety and the safe use of ICT. This understanding is incorporated into our staff training, so that we all remain vigilant to identifying the additional vulnerabilities for these children in our care.
- At the beginning of each academic year the first computing learning unit focuses upon online safety for all year groups (Y1 – Y6).
- Within each Computing unit throughout the year, teachers make explicit online safety links to support children apply their learning whilst online.
- Each year the school celebrates safer internet day.

Staff and the online safety policy

- All staff must sign the Staff Acceptable Use Policy on an annual basis, via CPOMS.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- All members of staff are aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

Parents and the online safety policy

- All parents, when their child joins the school, will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's online safety guidelines and within the constraints detailed in the school's online safety policy.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used on the school website.
- Parents are encouraged to look at the school's online safety policy and the pupil Acceptable User Agreement.
- Parents receive an online safety update in the school newsletter when appropriate.
- Parents are given information about what the school asks children to do online, including the sites they will be asked to access
- Workshops are organized where possible within school for parents to support their child/ren's online safety.

The Learning Platform and other home/school internet use

- All staff have been trained and given advice on how to effectively use Sharepoint, CPOMS and Arbor.

- Parents will be informed about what Sharepoint is and how it can enhance the learning of

- each child. All children will be given training on how to effectively use Sharepoint.
- All children will be given a username and password to access secure resources and facilities on Sharepoint .
 - Sharepoint will be regularly monitored for incidents of cyberbullying, inappropriate use of language or the uploading of inappropriate files. Children will be informed that the sending

of messages through Sharepoint is monitored and misuse of the messaging system will result firstly in a warning, followed by removal as a user from Sharepoint should such behaviour be repeated.

- Class teachers will monitor the use of Sharepoint. Any misuse of Sharepoint –will be reported to the Headteacher.

Monitoring and review

- This policy is implemented on a day-to-day basis by all school staff and is monitored on an annual basis by the online safety leaders. (Emma Carey and Tiana Moore).
- The Online Safety Leaders will carry out an audit each Autumn term of practices and make recommendations to the SLT if necessary.
- This policy is the Governors' responsibility and they will review its effectiveness annually. They will do this during reviews conducted between the online safety leader and/ or Designated Safeguarding Lead. Ongoing incidents will be reported to the Local Committee.
- Reviewed: September 2026