Aldborough Primary School
On-line Safety Policy

This Aldborough Primary Policy applies to all stakeholders.

DATE OF GOVERNOR APPROVAL	Autumn 2026
REVIEW FREQUENCY	Annually
REVIEW DUE	Autumn 2027
STATUTORY REQUIREMENT	YES

AMENDMENTS

Date	Summary of Amendment/s
12.12.2019 Full update of policy to meet current legislation.	Comply with KCSIE 2019 Equality Impact Assessment completed
05.11.2020	Update of Covid 19 section and Remote Learning Policy - CC
Autumn 2021	Update of policy to reflect changes to KCSIE 2021 Equality impact assessment completed.
Autumn 2022	Update of roles within school. Update to reflect changes to KCSIE 2022. Removal of Covid information.
Autumn 2023	Update roles within the school. Update to reflect changes to KCSIE 2023 re filtering and monitoring Update policy to reflect use of mobile phones by children and staff

	Change of title to ‘On Line Safety Policy’
Autumn 2024+ Autumn 2025	No Changes necessary
Autumn 2026	Links to Mobile Phone Policy 2026 added

Contents

1. Aims 4
Legislation and guidance 4
2. Roles and responsibilities 5
3. Educating pupils about online safety 7
4. Educating parents about online safety 8
5. Cyber-bullying 8
6. Acceptable use of the internet in school 10
7. Pupils using mobile devices in school 10
8. Staff using work devices outside school 10
9. How the school will respond to issues of misuse 10
10.Training 11
11. Monitoring arrangements and records 12
12. Links with other policies 12
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers) 13
Appendix 2: KS2 acceptable use agreement (pupils and parents/carers) 14
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors) 16
Appendix 4: online safety training needs – self audit for staff 17
Appendix 5: online safety incident report log 19
Appendix 6: responding to e-safety incidents concerning children 17

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology including the use of mobile and smart technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Online Safety

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- Contact: being subjected to harmful online interaction with other users; for example: 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; for example, 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. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

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
- Searching, screening and confiscation

It also refers to the Department'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.

2. Roles and responsibilities

2.1The Governing Board

The Governing Board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

Each term the Safeguarding Governor will meet with the Headteacher (also DSL) where online safety will be reviewed and the monitoring of online safety logs will be shared.

Safeguarding governor: Mrs Jan Legge

All governors will:

- Ensure that they have read and understand this policy
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

2.2 The Headteacher

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

2.3 The designated safeguarding lead

Details of the school's DSL and deputy are set out in our child protection and safeguarding policy as well as relevant job descriptions.

DSL (also Headteacher): Mrs Helen Bearman

Deputy DSL: Mr Courtenay Caston (from October 2022)

Deputy DSL: Mrs Rebecca Gale (from July 2023)

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

- ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Taking lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).
- 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
- To manage all online safety issues and incidents in line with the school child protection policy
- Providing regular reports on online safety in school for the Governing Board

This list is not intended to be exhaustive.

2.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 regular security checks and monitoring the school's ICT systems. 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's Behaviour policy

This list is not intended to be exhaustive.

The Head teacher / DSL and IT manager together will be responsible for:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provision at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet their safeguarding needs.

2.5 All staff and volunteers (if appropriate)

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
- Understand their roles and responsibilities in relation to filtering and monitoring and who to contact with concerns.

This list is not intended to be exhaustive.

2.6 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child understands and has agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2, age appropriate)

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 factsheet - Childnet International

2.7 Visitors

On occasions visitors may access the school's ICT systems or internet. When they do so they 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).

3. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

From September 2020 all schools will be required to teach:

- Relationships education and health education in primary 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 primary school**, 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
- how to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- what sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- how people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

4. Educating parents about online safety

We will communicate with parents and carers to raise awareness of online safety and reinforce the importance of children being safe online through letters or other communications home, and in information via our website.
This policy will also be shared with parents.

Online safety will also be covered during cluster events and annually in school Internet Safety evenings.

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

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

5. Cyber-bullying

5.1 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's Keeping Children Safe and Behaviour policies.

5.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know

how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.

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 posts information on cyber-bullying to parents via the Online Safety section of the school's web site so that they are aware of the signs, how to report it and how they can support children who may be affected.

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.

5.3 Examining electronic devices

Children at Aldborough Primary School are not allowed to bring personal electronic devices or mobile phones into school unless agreed by the Head teacher in exceptional circumstances (see Mobile Phone Policy 2026).

However, school staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

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 whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (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 in line with the filtering and monitoring standards.

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

7. Pupils using mobile devices in school (see Mobile Phone Policy 2026)

Pupils are only allowed to bring mobile devices into school in exceptional circumstances and with the agreement of the head teacher. Any mobile phones brought into school must be kept in the school office throughout the school day and children are not permitted to use them on school premises.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school Behaviour policy.

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

UKCIS guidance on sharing nudes and semi-nudes

8. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

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

Work devices must be used solely for work activities.

9. 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 appendix 6. 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 which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

10. Training

All staff will receive appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – see para 141 of KCSIE for further information) at induction. The training will be regularly updated. In addition, all staff will receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.

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).

Staff should be made aware that:

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

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

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

of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Keeping Children Safe policy.

11. Monitoring arrangements and records

The DSL logs Behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed annually by the ICT Manager and the Computing subject leader. At every review, the policy will be shared with and approved by the governing board.

See Keeping Children Safe policy for details of records and information sharing relating to safeguarding concerns.

NB FROM OCTOBER 2022 WE WILL BE CHANGING OUR RECORDING SYSTEM TO CPOMS. ALL STAFF WILL RECEIVE THE NECESSARY TRAINING TO USE THE ONLINE SAFEGUARDING SYSTEM FOR RECORDING CONCERNS.

12. Links with other policies

This online safety will be reviewed every year and is linked to our:

- Keeping Children Safe policy
- Behaviour & Anti-Bullying policy
- Data protection policy and privacy notices
- Complaints procedures
- Mobile Phone Policy

Appendix 1: EYFS and KS1 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 ∑ I will 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 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 for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2 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:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** ∑ Always use the school's ICT systems and the internet responsibly and for educational purposes only ∑ Only use them when a teacher is present, or with a teacher's permission ∑ Keep my username and passwords safe and not share these with others ∑ Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer ∑ Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others ∑ Always log off a computer when I'm finished working on it **I will not:** ∑ Access any inappropriate websites including: social networking sites, chat rooms, gaming sites or sites which show intolerance of others (Prevent) unless my teacher has expressly allowed this as part of a learning activity ∑ Open any attachments in emails, or follow any links in emails, without first checking with a teacher ∑ Use any inappropriate language when communicating online, including in emails ∑ Log in to the school's network using someone else's details ∑ Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I will not bring a personal mobile phone or other personal electronic device into school unless it has been agreed by the head teacher. Any mobile phone or electronic device will be stored in the school office throughout the school day.** ∑ I will not use it on the school premises **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's 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 for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**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 linked to radicalization or extreme views (Prevent strategy) (or create, share, link to or send such material) ∑ Use them in any way which could harm the school's reputation ∑ 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 **If I bring a personal mobile phone or other personal electronic device into school:** ∑ I will not use it on the school premises other than to double authenticate CPOMS or in the staff room.	
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:	**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?	
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?	
Are you aware of the ways pupils can abuse their peers online?	
Are you aware of the government's Prevent strategy and how radicalization can be promoted through online activity?	

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix 6: responding to e-safety incidents concerning children

Flowchart for responding to e-sa-fety incidents concerning children

