ALDERMAN RICHARD HALLAM PRIMARY SCHOOL

Online Safety Policy

Policy Reviewed: September 2025

Online Safety Policy

The Online Safety leads are Mr W Holder and Miss L Ellis. Online safety is overseen by Mrs C Lawes, the school's Designated Safeguarding Lead.

Our Online Safety Policy has been written by the school, building on government guidance including Keeping Children Safe in Education's 4Cs (Part 136) relating to online safety. The school will use dynamic risk assessing and take actions as appropriate to continually help shape and support this policy as is pertinent to the needs of the school. It has been agreed by the Senior Leadership Team and approved by governors.

Teaching and Learning

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and is a necessary tool for staff and pupils.

Internet use will enhance learning

- The internet access within school will be designed expressly for pupil use and will include filtering appropriate to the age of pupils (ekte Primary Pupil Level).
- Pupils will be taught what internet use is acceptable and unacceptable, and given clear guidelines for internet use.
- Pupils will be educated about the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught how to evaluate internet content.
- The school will ensure that the use of internet-derived materials by staff and pupils complies with copyright law – including law regarding new and emerging technologies such as AI.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught to report unpleasant internet content or any content that worries them.
- Pupils will be taught about internet-enabled devices and how all devices, apps or programs on the internet need to be used appropriately and safely.
- Online safety lessons will encompass the 4Cs from KCSiE 2025: Content, contact, conduct and commerce to ensure children are aware of the dangers but also opportunities that are online.

Internet Access Policy Statement

All internet activity should be appropriate to staff's professional judgement, based on the teacher's code of conduct (http://www.gtce.org.uk/teachers/thecode/) and the children's education. Internet activity should be in line with the following:

- All usernames and passwords are to be kept strictly private and not shared with other individuals;
- The internet may be accessed by staff throughout their hours in school and at home;
- Activity that threatens the integrity of the school's computer systems, or that attacks or corrupts other systems, is strictly prohibited;
- Users are responsible for all email sent and for contacts made that may result in email being received. Due regard should be paid to the content. The same professional levels of language should be applied as for letters and other media – please contact Mr W Holder if you are unsure of potential threats to the network;
- Use of the school's internet for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is prohibited;
- Copyright of materials must be respected. When using downloaded materials, including free materials, the Intellectual Property rights of the originator must be respected and credited. All material saved on the school's network is the property of the school and making unauthorised copies of materials contained thereon may be in breach of GDPR, Individual Copyright or Intellectual Property Rights;
- Use of materials stored on the school's network for personal financial gain is prohibited;
- Posting anonymous messages and forwarding chain letters is prohibited;
- The use of the internet, email, or any other media to access inappropriate materials such as pornography, racist or any other offensive material is forbidden;
- All web activity is monitored, including the content of email, therefore it is the responsibility of the user to ensure that they have logged off the system when they have completed their task;
- Children must not be given unsupervised access to the internet. For the purposes of this policy, 'supervised' means that the user is within direct sight of a responsible adult;
- The teaching of online safety as well as emerging technologies such as AI is included in the school's Computing and online safety progression documents, but all teachers within all year groups should be including internet safety issues as part of their discussions on the responsible use of the school's computer systems as per the SMART poster (children's online safety policy);
- All children must understand that if they see an unacceptable image or word on a computer screen, they must turn the screen off and report it immediately to a member of staff.

Internet and System Monitoring

Through the use of software provided by Smoothwall Monitor, all internet activity is monitored by the system. It is the responsibility of the Headteacher, the Deputy Headteacher, and the Designated Safeguarding Leads to review this activity periodically. It is the duty of the Business Manager to report any transgressions of the school's Online Safety Policy and/or use of obscene, racist or threatening language detected by the system to the school's SLT. Occasionally, it may be necessary for the Business Manager to investigate attempted access to blocked sites; this should be recorded in the I.C.T. violations register,

and SLT notified. DSLs will work together to ensure that monitoring and filtering is appropriate for the school.

All serious transgressions of the school's Acceptable Use Policy are recorded in the Business Manager's documents violations register, which is password protected, and SLT will be informed of the incident.

Transgressions of this policy and use of inappropriate language can be dealt with in a range of ways, including removal of network and internet access permissions. Staff will be reported to the Headteacher and will be dealt with according to the school's and LA's disciplinary procedures, or through prosecution by law.

Managing Internet Access

- School I.C.T. systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority and relevant organisations.

Email

- In email communication, pupils and staff must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how email from pupils and staff to external bodies is presented and controlled; in the majority of cases, emails to external bodies should be sent from staff email accounts.
- The forwarding of chain letters is not permitted.

Published Content and the School Website

- Staff or pupil personal contact information will not be published. The contact details given online will be for the school office.
- The Senior Leadership Team will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupil's Images and Work

The school's aim is for the website to reflect the diversity of activities, individuals and education that can be found at Alderman Richard Hallam Primary School. However, the school recognises the potential for abuse that material published on the internet may attract, no matter how small this risk may be. Therefore, when considering material for publication on the internet, the following principles should be borne in mind:

- No video recording or photograph may be published without the written consent of the parents or carers of the child concerned, and the child's own verbal consent (See ARH GDPR consent form);

- Surnames of children should not be published, especially in conjunction with photographic or video material;
- No link should be made between an individual and any home address (including simple street names);
- Where the person publishing material suspects that there may be child protection issues at stake, then serious consideration must be taken as to whether that material may be published or not. In the case of a simple piece of artwork or writing, this may well be fine, but images of that child should not be published. If in any doubt at all, this should be referred to one of the school's Designated Safeguarding Leads.

School Networking and Personal Publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved e.g. Newsround.
- Pupils will be advised to never give out personal details of any kind which may identify them, their friends or their location.
- Pupils, parents and carers will be advised that the use of social network spaces outside school brings a range of dangers for primary-aged pupils.

Managing Filtering

- The school will work with the ekte and Smoothwall, to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable online materials, the site must be reported to the Online Safety leads (Miss L Ellis and Mr W Holder).
- DSLs will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing Video-conferencing and Webcam use

- Video-conferencing should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a video-conference call.
- Video-conferencing and webcam use will be appropriately supervised for the pupils' age.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. The Senior Leadership Team should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications. Mobile phones should not be brought into school and should be sent to the school office to be collected by parents or carers. In some cases, (e.g. a child walking home alone), children may hand in their mobile phones to their class teachers for safe keeping at the start of the day in line with our Mobile

Phone Policy. These will be returned to the pupils at the end of the day. Other technologies, such as AI to support teaching and learning, will be evaluated on an individual basis.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school (See Seesaw Policy).

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to GDPR. Please see the Data Protection Policy for further information.

Authorising Internet Access

- All staff must read and sign the Staff Code of Conduct and Acceptable Use Policy before using any school I.C.T. resource. The school will maintain a current record of all staff and pupils who are granted access to school I.C.T. systems. A message displaying this information is shown when logging onto any school computer.
- In Key Stage 1, access to the internet will be led by adult demonstration with directly supervised access to specific, approved online materials. Some researching techniques will be used in KS1 but staff must conduct searches beforehand and must provide example websites to begin with.
- Parents and carers will be asked to sign and return a consent form to allow their child to access any internet enabled device.
- Any person not directly employed by the school will be asked to sign an acceptable use of school I.C.T. resources form before being allowed to access the internet from the school site.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor the Local Authority can accept liability for any material accessed, or any consequences of internet access.
- The school will audit I.C.T. use to establish if this policy is adequate and that its implementation is appropriate and effective.

Handling Online Safety Complaints

- Complaints of internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse **must** be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school's Safeguarding and Child Protection Policy and safeguarding procedures.
- Pupils, parents and carers will be informed of the complaints procedure (see the school's Complaints Policy).
- Pupils, Parents and carers will be informed of consequences for pupils misusing the Internet.

Introducing the Online Safety Policy to Pupils

- Online safety rules will be shared in all rooms where computers are used and discussed with pupils regularly (SMART posters – the child-friendly online safety policy displayed in classrooms or on flipcharts).
- Pupils will be informed that network and internet use will be monitored and appropriately followed up.
- Staff training on online safety will be shared by the Online Safety Leads. If any staff members require additional training, please contact Miss L Ellis or Mr W Holder.
- Online safety training will be embedded within the school's Computing and Online Safety progression documents as well as routeways, the Personal, Social and Health Education (PSHE) curriculum and the Behaviour and Safety curriculum.

Staff and the Online Safety Policy

- All staff will be given access to this policy and its importance explained.
- Staff will be informed that the network and internet traffic is monitored and can be traced to individual users.
- Staff that manage filtering systems or monitor I.C.T. use will be supervised by the Senor Leadership Team and work to clear procedures for reporting issues.

Enlisting Parents' and Carers' Support

Parents' and carers' attention will be drawn to this policy in the latest news emails. The school will ask all new parents or carers to sign the parent pupil **agreement when they register their child with the school. Internet access will also be covered as part of our consent forms.**
Parents and carers have access to the National College's 'National Online Safety' area to enable them to seek advice and training.

Home Learning

If required, home learning will take place online using Seesaw, Zooms and Teams according to the latest government guidance.

Policy Links
This policy is to be read in conjunction with the following other policies and documents:

- Mobile Phone Policy
- Acceptable Use Policy
- Social Media Policy
- Seesaw Policy
- Remote Learning Policy
- Safeguarding and Child Protection Policy
- Data Protection Policy