Avondale Primary School

Online Safety Policy

This policy was reviewed by V Brown, B Laycock and S Speakman
Reviewed September 2024
Will be reviewed in September 2025

"For learning, smiling and remembering"

INTRODUCTION

The resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies. Use of the Internet, by its nature, will provide access to information, which has sometimes not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times they will be able to move beyond these to sites unfamiliar to the teacher. There is therefore the possibility that a pupil may access unsuitable material either accidentally or deliberately.

The purpose of this policy is to:

 Establish the ground rules we have in school for using the Internet.

 Describe how these fit into the wider context of our behaviour and PHSE policies.

 Demonstrate the methods used to protect the children from sites containing unsuitable material.

This policy deals specifically with the educational and curriculum element of online safety. Guidance and procedure relating to infrastructure, networking and appropriate use of technology by staff are contained in the ICT acceptable use policy. Our online safety Policy has been written by the school, building on the Blackburn with Darwen policy guidance. It has been agreed by the senior leadership team and approved by Governors. It will be reviewed annually.

The school believes that the benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians.

At Avondale Primary School we feel that the best recipe for success lies in a combination of educating children about how to keep safe, site-filtering, appropriate supervision and by fostering a responsible attitude in our pupils in partnership with parents.

Writing and reviewing the online safety policy

The online safety Policy relates to other policies including those for Computing, ICT acceptable use, data protection, anti-bullying, behaviour and safeguarding.

- The Headteacher is the online safety lead and designated safeguarding lead.
- The online safety Policy was revised by Mrs V Brown, Mr B Laycock and S Speakman

Why the Internet and communication technology use is important

'Technology offers unimaginable opportunities and is constantly evolving. Access is currently becoming universal and increasingly more mobile, and pupils are using technology at an ever earlier age…' Ofsted

The safe use of technology is a part of the statutory curriculum and the internet a necessary tool for staff and pupils.

Ofsted guidance for schools recommends that all schools:

- provide an age-related, comprehensive curriculum for online safety that enables pupils to become safe and responsible users of new technologies
- audit the training needs of all staff and provide training to improve their knowledge of and expertise in the safe and appropriate use of new technologies

- work closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at school
- use pupils' and families' views more often to develop online safety strategies.

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- Educational and cultural exchanges between pupils worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across networks of schools, support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with Local Authority and DFE;
- Access to learning wherever and whenever convenient.

School and community involvement in online safety policy and practice

At Avondale School we believe that by involving representatives from all the school community in evaluating, formulating and reviewing online safety policy and practice, our children, staff and governors will be the safest they possibly can be.

Involving children in policy, practice and educating others

The school has a number of pupils in school who are digital leaders. Part of their role is to contribute to online safety policy and practice and inform parents and peers of online safety issues on a regular basis.

Leadership of online safety

Our online safety leads are Mrs V Brown, Mrs Wright and Mrs S Speakman

The responsibilities of the online safety lead are to:

- Maintain own knowledge of wider online safety and online safety leadership through training, seeking advice, and signing up to regular updates
- Carry out an online safety audit to inform the review process
- Regularly review the effectiveness of online safety policy and practice
- With the computing subject lead, ensure the computing curriculum is progressive and age appropriate and that there are opportunities across the wider curriculum including PSCHE to reinforce online safety messages.
- Ensure all school staff receive online safety training, at least every 2 years, and that a record of training is maintained
- Provide updates on online safety policy and practice to governors
- With the school's technical support, ensure that appropriate filtering and anti-virus software is in place
- Maintain reporting procedures for online safety incidents - This may be part of a wider reporting system, but should include access to inappropriate resources (intentional or otherwise), inappropriate use of school technology, online safety and cyberbullying disclosures. There should also be a record of how it was dealt with and any consequences e.g. additional online safety input; discussion with parents restricting access etc.
- Provide or source online safety information and training for parents

- Ensure that appropriate acceptable use agreements are signed by pupils and parents and that permission for use of images and video is sought from parents (and pupils when appropriate)
- Ensure that the educational potential and possible online safety issues are investigated before using new technology.
- The head teacher and at least another member of the SLT should be aware of the procedures to be followed in the event of a serious online-safety allegation being made against a member of staff.
- Annually review the schools online safety strategy, policy and practice

Governors

The role of the online safety governor will include:

- Regular meetings with the DSL or deputy and online safety co-ordinator
- Regular monitoring of online safety incident logs
- Reporting back at Governor meetings

MANAGING INFORMATION SYSTEMS

How will information systems security be maintained?

- Virus protection will be updated regularly.
- Personal data sent over the Internet will be encrypted.
- Portable media may not be used without specific permission followed by a virus check.
- Unapproved software will not be allowed in pupils' work areas or attached to email.
- Portable drives should not be used in school computers.
- Whole class or teacher email addresses will be used at Avondale for communication outside of the school by children.
- Pupils may only use approved email or blogging accounts.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Access in school to external personal email accounts may be blocked.
- The forwarding of chain messages is not permitted.
- Parents should email staff via the school office
- Staff should only use school email accounts to communicate with pupils as approved by the Senior Leadership Team
- If staff need to work from home for a 14 day period then there will be devices that can be loaned from school that will be able to access the school network remotely. These need to be returned upon the staff's member return to work.
- Teaching staff have been provided with a laptop and a mobile phone for school use, this can be used, on Wifi, in school and from home. These phones have no SIM and thus no number, so they can only be used on Wifi
- Any personal mobile phones used in school must be used on the school wi-fi. Visitors should use the Guest Wi-Fi.

Online safety Education and Training

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience. Current guidance stipulates that it is not sufficient to keep pupils safe in school. It is our responsibility therefore, to ensure they have opportunities to learn how to stay safe and deal with the risks associated with the internet

and communication technology in the world around them. Keeping our children safe involves educating all members of our school's community, including governors, parents and all staff working in school.

Educating pupils

Our online safety curriculum

At Avondale School we ensure that children have access to a progressive online safety curriculum across all year groups. There is a half term dedicated specifically to teaching Online Safety (usually at the start of the year) and it is also woven throughout the curriculum in other areas.

Early Years Foundation Stage, Early Learning Goal

Children recognise that a range of technology is used in places such as homes and schools. They select and use technology for particular purposes.

In order to safely select and use technology we believe that children in the Foundation Stage need to be taught an age appropriate online safety curriculum. During the Early Years Foundation Stage we will ensure our children use technology safely so that by the time they leave the Foundation Stage they are ready to access the key stage 1 curriculum

The National Curriculum 2014 for Computing stipulates that pupils:

- In key stage 1 are 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.
- In key stage 2 are taught to use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

At Avondale School we use a number of approaches to ensure our pupils are confident and safe users of technology in and out of school.

To ensure pupils have access to an age-appropriate online safety curriculum that is flexible, relevant and engages pupils' interest; that is used to promote online safety through teaching pupils how to stay safe, how to protect themselves from harm, we:

- Introduce age appropriate school and classroom rules each year and reinforce them regularly
- Ensure children know the SMART acroymn (Safe, Meeting, Accepting, Reliable, Tell)
- Use progressive statements within the Computing curriculum scheme of work, to ensure that areas of online safety relating to communication, information, creating and presenting ideas, and Computer Science are covered regularly. These are planned into either computing, PSHE or the general curriculum as appropriate. The Computing scheme can be found on the curriculum in the Reading At The Heart Of The Curriculum area in Teacher Shared.
- Deliver online safety messages in assembly in response to need, to reinforce national initiatives and agendas such as Safer Internet Day and Anti-Bullying Week.
- Before using a new device or online resource, pupils are taught how to use it safely and appropriately. This is reinforced regularly.
- Teach pupils to tell a trusted adult should they be worried of upset by anything they encounter online or using communication technology. (All staff are made aware of what to do should if a pupil confides in them.)

The need to keep login details and other personal information private will be reinforced regularly when using the schools network, learning platform and any other methods of communication agreed by the headteacher.

Pupils will be taught how to evaluate Internet content appropriate to their age.

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught what Internet use is responsible and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation appropriate to their age group.
- Pupils will be taught about the dangers of radicalisation and extremism at an appropriate level for their age.
- Pupils are taught to be SMART (Safe, Meeting, Accepting, Reliable, Tell)

Educating parents

Children often seem more at home in the digital world than their parents. To ensure that children are the safest they possibly can be, we must educate parents about the risk of using the internet and communication technology for their children and the potential for their own use of technology to place themselves or their child at risk.

We ensure parents receive information and training by:

- Providing links to information and resources for parents on our school website
- Providing regular updates to parents through newsletters
- Including face to face opportunities. e.g. Inviting parents to online safety workshops, inviting parents to join online safety sessions in class or attend online safety assemblies.
- Encouraging parents to act as role models when using technology

The school will share with parents and children, our belief that:

- The unsupervised use of social network spaces intended for adults outside school is inappropriate for pupils of primary age.
- Family friendly filtering can help to keep children safe, however education and the opportunity to develop safe practice is essential for keeping children safe
- Pupils who use the internet and other communication technology may be at risk of being groomed or radicalised. It is important that parents understand that secrecy is a possible factor in both of these.
- What pupils do online now, can affect their future life.
- If a child is happy to tell a parent or carer when they are worried, they are the safest they can possibly be; therefore, we encourage parents to nurture a sense of trust between them and their child when talking about using technology.
- Children are also encouraged to report their concerns via a member of staff or trusted adult.

Educating staff and the wider school community

- We ensure that all new staff receive online safety training as part of their induction
- All school staff have access to basic online safety training regularly

- The online safety lead and key members of the online safety group have access to a higher level of training, updates and information to ensure that have the skills and knowledge necessary to lead all areas of online safety. Basic training includes
- Online safety issues for pupils
- Reporting procedures
- Guidance on appropriate use of communication technology by staff and pupils
- Guidance for staff on how to stay safe
- Expectations in terms of passwords and data security
- Expectations in terms of professional conduct including the use of social media
- Teaching pupils to minimise the screen if they see something that makes them feel uncomfortable.

Online safety training references and complements guidance in the Safer Working Practices document.

Social networking, social media and personal publishing

- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction.

Twitter and Facebook

The school Twitter account is used by Mr Clegg for Sports News.

Mrs Speakman posts to the main school Facebook accounts and has overall control and editing responsibilities. Miss Johnson & Mr Clegg and Mrs Speakman also have a logins for Facebook and can create posts. Mrs Speakman monitors the content of the Twitter & Facebook accounts and should there be any unwanted communication the Online Safety policy will be followed. The use of images and children's names are not allowed and follows the same protocol as specified in the Online Safety policy.

Keeping staff and pupils safe in school

All access to the internet is filtered by Fortinet. The school will work with the Schools Broadband, and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the online safety Lead who will inform the LA ICT team and Schools Broadband so that they can take appropriate action.

All users will be taught how to care for devices in terms of health and safety. This includes avoiding placing food or liquids near to electrical devices, carrying equipment and rules around charging and electrical sockets.

The school internet access is designed expressly for pupil use and includes appropriate filtering.

A suspicious search filter is sent daily to the Computing Technician and Headteacher.

If staff or pupils discover unsuitable sites, the URL will be reported to the School online safety co-ordinator who will then record the incident and escalate the concern as appropriate.

Sanctions for inappropriate use of the internet and communication technology will be explained to the children. A record of any misuse in school will be kept in the computer suite.

At Avondale School staff do not use their own personal devices/accounts to contact parents and pupils. The school text messaging service is used to contact parents when on trips and visits and the school email address should be used when communicating with parents. IPADS and phones are provided for recording school related activities. Images of children should not be stored on personal devices.

Acceptable use agreements

- A home school agreement, which includes information re access to the internet and communication technology will be signed by pupils and parents on entry to school in EYFS and re-issued as children enter KS2
- Class rules agreement are displayed in class and adhered to
- An acceptable use agreement for school staff is signed annually

Passwords security

Pupils are encouraged to keep their password private. Parents are encouraged to ask children to logon to their accounts and show them what they have been doing rather than ask children to share their passwords.

- Pupils in Reception have a class login and password whereas children in Years 1, 2. 3, 4, 5 & 6 have their own individual login and passwords.
- Pupils will be taught to tell an adult immediately about any offensive communications they receive or any inappropriate content they may encounter using digital technology.
- Children will be taught to tell a member of staff immediately should they encounter anything that makes them feel uncomfortable. Our SMART rules are revisited every computing session.
- Pupils may only use approved digital methods of communication on the school system. E.g. communication tools in the Learning platform, Purple Mash and Google Classroom.
- Pupils in key stage 2 upwards will be taught about the report abuse button (this can be found on many websites including our school website)
- Pupils and staff will use equipment responsibly.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location or arrange to meet anyone without specific permission.
- Staff passwords for email accounts are changed every 30 days, whereas passwords for computers are changed at least every 60 days.

Reporting online safety concerns

Children are encouraged to report their concerns via a member of staff. We also encourage the children to use national resources such as childline and CEOP

- A record of online safety incidents is kept in on CPOMS.

- The nature of the incident and action taken are recorded with and any consequences e.g. additional online safety input; discussion with parents restricting access etc. This includes access to inappropriate resources (intentional or otherwise), inappropriate use of school technology, online safety and cyberbullying disclosures.

Cyberbullying

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti - bullying and behaviour. There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded on CPOMs
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

Other Online Safety Issues

- Sexting – Children in Year 5 and 6 will be informed during their online-Safety lessons about the implications of sexting and how, once a picture has been sent, this image can never fully be removed from the world wide web.

- Pornography – many children will come across some type of pornographic content when searching the Internet. Children are taught about what to do if they come across this type of material and who to speak to.

- Radicalisation is defined as the act or process of making a person more radical or favouring of extreme or fundamental changes in political, economic or social conditions, institutions or habits of the mind.

- Extremism is defined as the holding of extreme political or religious views.

Radicalisation and Extremism - Avondale is fully committed to safeguarding and promoting the welfare of all its children. As a school we recognise that safeguarding against radicalisation is no different from safeguarding against any other vulnerability. The school has a zero tolerance approach to extremist behaviour for all school community members. We rely on our strong values to steer our work and ensure the pastoral care of our children protects them from exposure to negative influences.

The school through its training cycle are aware that the internet and in particular social media is being used as a channel to influence and in extreme cases radicalise children and young people. Furthermore the school is aware that vulnerable children can be exploited and groomed by older young people and adults and will:

- Consider and discuss the threats from radicalization and extremism.
- Ensure that the understanding of radicalisation is embedded in safeguarding practice and that PREVENT coordinators are engaged and signposted.
- Consider how the threat of radicalisation through the Internet and Social Media is being addressed
- Review the Online Safety education in light of these widening and extreme risks.

At Avondale all staff and children are expected to uphold and promote the fundamental principles of British values, including democracy, the rule of law, individual liberty and mutual respect, and tolerance of those with different faiths and beliefs.

 Children are encouraged to adopt and live out our Core Values. These complement the key "British Values" of tolerance, respect, understanding, compassion and harmonious living.
 Children are helped to understand the importance of democracy and freedom of speech,
 Children are supported in making good choices from a very young age, so they understand the impact and consequences of their actions on others.

Published content

Any information that can be accessed outside the school's intranet should be classed as published whether in electronic or paper format.

- Electronic communication sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- General contact details should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. (This may be through education and guidance, as directly reading everything is impractical)
- Where pupils publish work, there will be systems in place to check the content and pupils will be given clear guidelines about what can be published.

Publishing pupil's images and work

- Staff and pupils using digital cameras, video recorders or sound recorders will ensure that they inform others before recording them and always use equipment in a respectful manner. (In the Foundation Stage this may not be practical when capturing a child in the process of learning, however should be modelled as often as possible.)
- Photographs that include pupils will be selected carefully
- Pupils' full names will not be used anywhere in association with photographs.
- Written permission from parents or carers will be obtained before photographs or video of pupils are published.
- Where pupil's work is published the school will ensure that the child's identity is protected.
- Where school events are being publicised, care will be taken not to reveal information that may put children or staff at risk e.g. the date and location of a trip

Guidance for taking photographs and video during school performances and assemblies.

Information Commissioner's Office
http://www.ico.org.uk/for_organisations/sector_guides/~/media/documents/library/Data_Protection/Practical_app lication/TAKING_PHOTOS_V3.ashx

Managing emerging technologies

- The educational benefit of emerging technologies and any potential risks will be considered and shared with staff before they are used in school.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Responsible ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Parents will be asked to sign and return a consent form for their children to access the internet.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor Schools Broadband can accept liability for the material accessed, or any consequences of Internet access. Any inappropriate access whether intentional or unintentional will be reported to the e safety co-ordinator and to the LA where necessary.
- The school will audit ICT provision to establish if the online safety policy is adequate and that its implementation is effective.

Handling online safety complaints

- Complaints of Internet misuse will be dealt with, inline with the complaints policy, by the Headteacher and where appropriate inform the governing body and/or the local authority
- Any complaint about staff misuse must be referred to the Headteacher who will refer to the staff behaviour policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure on request.

Communications Policy Introducing the online safety policy to pupils

- Online safety rules will be posted in all rooms where pupils may access the internet and discussed with the pupils at the start of each year. Where possible images and symbols will be used to help make them accessible to young children.
- Pupils will be informed that network and Internet use will be monitored and can be monitored and traced to the individual device or login.

Introducing the policy to parents

Parents' attention will be drawn to the School online safety Policy and practice:

- in newsletters,
- in the school brochure
- on the school website

Staff and the online safety policy

- All staff will be given the School online safety Policy and its importance explained.
- Staff should be aware that internet traffic may be monitored and traced to the individual device or login. Discretion and professional conduct is essential.
- The school may use monitoring software where this is available to ensure that inappropriate materials are not being stored or used on school equipment.