

The Avenue Primary School

E– Safety & Acceptable Use Policy July 2018

To be reviewed annually: July 2019



E-Safety Policy/ Acceptable User Policy

Introduction

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and electronic publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to make safe and responsible decisions in order to control their online experience.

At The Avenue Primary, we understand the importance of effective e-safety practice for both staff and pupils and this policy sets out how we ensure this is achieved.

The school's e-safety/AU policy operates in conjunction with other policies including Curriculum policies and Data Protection.

E-Safety in school

E-safety depends on effective practice at a number of levels:

- Responsible use of technologies by all staff, pupils and governors; encouraged by the curriculum and made explicit through published policies.
- Sound implementation of the E-safety/Acceptable Use Policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering systems.

1.0 School e-safety/AU policy

1.1 Writing and reviewing the policy

This Policy relates to other policies including those for data and for child protection.

- The school has appointed a designated safety lead, the Head Teacher Emma Yule. Other members of the team include Grahame Pennock and Jayne Booth. The Chair of Governors is also a member.
- Our E-Safety/ AU Policy has been written by the school. It has been agreed by the staff and governors.
- The E-Safety/AU Policy will be reviewed in annually, each December

1.2 Teaching and learning

1.2.1 Why Internet use is important

- 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 curriculum and a necessary tool for staff and pupils.

1.2.3 Internet use will enhance learning

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils.
- Pupils will be taught what Internet use is acceptable and what is not, and will be given clear objectives for Internet use, using the SMART rules (See Appendix 2).
- Internet access will be planned to enrich and extend learning activities.
- Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.2.4 Pupils will be taught how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported designated safety lead.
- Staff should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and be shown how to validate information before accepting its accuracy.

1.2.5 When will children have direct access to the Internet?

- Online content (e.g. CBeebies) will often be used by the teachers for specific tasks (see Appendix 1 for examples). In these situations, the children are not searching the internet or navigating away from the page/s and tasks that have been set. Teachers will have spent a reasonable length of time previewing the site to ensure that it matches the learning outcomes of the lesson/setting.
- Searchable cached sites such as Espresso or Purple Mash will allow access within a site but not beyond it.
- Children from Year 5 onwards may use a safe search engine when searching for information. This is not a failsafe way of preventing access to inappropriate sites but is a good line of defence. Searches will only be permitted when a member of staff is present. Where possible, teachers should have pre-searched for the topic in hand and previewed the hits that will be used based on the fact that search engines do not necessarily give the most appropriate site at the top of their lists.
- Children in Y5 and Y6 may be given permission in small groups to independently research using the internet.
- In most cases, to avoid fruitless hours of browsing, a key website/s will be identified by the teacher for the children to use to find information
- Searches for images via google, yahoo etc. are not blocked and should be monitored.

1.3 Managing Internet Access

1.3.1 Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly by OneIT.
- The school uses broadband with an effective firewall and filters. A smooth wall is incorporated into the network which is managed by OneIT. More information about the smooth wall can be gained from the Head Teacher.

1.3.2 E-mail

- Children are not allowed access to personal e-mail accounts or chat rooms whilst in school, unless they are located on the school network.
- The forwarding of chain letters is not permitted.
- The children will not be given a school email account but will be made aware of email use through simulations, for example E Mail Detectives.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. With the exception of the Head Teacher, staff or pupils personal information will not be published.
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The office staff will also have access in order to update specific areas.

1.3.3 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site, or on the school Twitter account, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site, or the school Twitter account.
- Pupil's work can only be published with the permission of the pupil and parents.

1.3.4 Social networking and personal publishing

- Social networking sites and newsgroups will be blocked for pupils, unless a specific use is approved.
- Pupils are taught never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc. (See Appendix 2 - The SMART Rules).
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils as many have age restrictions.
- Parents are informed that school take no responsibility for issues which arise from social media outside of school.

1.3.5 Managing filtering

- The school will work in partnership with the service provider, currently OneIT, to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school Safeguarding Lead – Emma Yule or Jayne Booth.
- OneIT will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.3.6 Managing emerging technologies including Mobile phones

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used on the school grounds by pupils at The Avenue Primary. The sending of abusive or inappropriate text messages on school grounds is forbidden and will be reported to parents and the Head Teacher.
- If a mobile phone is brought onto the school premises, it will be handed in immediately on arrival to the school office for safekeeping and collected on the way out of school at 3:15pm. It will not be stored in bags or pockets. Failure to observe these rules will lead to confiscation.

- Staff will not contact pupils using email or phone (mobile or land line). Parents will not be contacted by mobile phone unless urgent contact is required and for school business, e.g. an emergency with their child on a school trip.
- The wearing of Smart watches will not be permitted in school as they enable access to applications and text/ email messages.

1.3.7 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- All access to personal data will be password protected.

1.4 Policy Decisions

1.4.1 Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff, including Teaching Assistants and Supply Teachers must read and sign the E-Safety/ Acceptable User Policy (AUP) before using any school ICT resource (See Appendix 3).
- At FS/Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents and pupils will be asked to sign and return a consent form agreeing to comply with the school's Acceptable Use Policy (See Appendices 4 and 5).

1.4.2 Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The Head Teacher will ensure that the E-Safety/AUP Policy is implemented and compliance with the policy monitored.

1.4.3 Handling e-safety complaints

- Complaints of Internet misuse involving the pupils will be dealt with by a senior member of staff. Sanctions resulting may include interview/counselling by class teacher / Head Teacher; informing parents or carers; removal of Internet or computer access for a period of time.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

1.4.4 Community use of the Internet

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

1.5 Communications Policy

1.5.1 Introducing the E-safety/Acceptable User Policy to pupils

- Rules for Internet access will be posted in all networked rooms – The SMART poster (See Appendix 2).
- The poster will become the wallpaper for log on screens as a regular reminder of the rules.
- Pupils will be informed that Internet use will be monitored.
- Advice on e-Safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use (See Appendix 1 for examples).

1.5.2 Staff and the e-Safety/ AU Policy

- All staff will be given the School E-Safety/Acceptable User Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will be given a “professional” email account.
- The staff are at liberty to use their accounts for correspondence between one another or other professional bodies as part of their work.
- Passwords must be changed by the user who agrees, through the staff agreement form, to keep passwords secret, even from their colleagues, family and friends.
- Users will also be expected to report any offensive emails that they receive to the head teacher. Any reports of offensive emails will be reported to the Head teacher. Users should also report any attempts by people who they don't know trying to contact them.
- School professional email accounts should not be used for personal communications; use is dedicated to educational matters only.
- Use of newsgroups or forums/chat rooms in school is not permitted unless located on the school network.
- The staff internet agreement form sets out the terms and conditions that they must agree to **before** being allocated an account. Failure to adhere to the agreement will result in referral to the Head teacher and possible disciplinary action. See Appendix 3.

1.5.3 Enlisting parents' /carers' support

- Parents/Carers attention will be drawn to the School E-Safety/Acceptable User Policy upon joining the school and if significant amendments are made.
- A school document 'A Parents' Guide to Video Games and Online Safety' will be issued to all new parents in school and be accessible through the school website (See Appendix 6).
- School, through the Head Teacher or Assistant Head Teacher, will contact parents where concerns have been raised about a pupil's access to age-inappropriate games, DVDs etc.

1.5.4 Signed Agreement

- Parents will be asked to sign the policy agreement on behalf of their children upon enrolment in the school. The agreements will be stored in a file in the school office until the child leaves.
- Staff will be asked to sign the agreement upon joining the school. These will be updated when significant changes are made to the policy. The signed agreements will be stored in a file in the school office.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	<p>Pupils should be supervised.</p> <p>Pupils should be directed to specific, approved on-line materials.</p>	
Using search engines to access information from a range of websites.	<p>Pupils should be supervised.</p> <p>Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.</p>	<p>Safe Search for Kids Ask Jeeves for kids CBBC Search</p>
Exchanging information with other pupils and asking questions of experts via e-mail.	<p>Pupils should only use approved e-mail accounts under direct supervision. All communication must be approved by an adult.</p> <p>Pupils should never give out personal information.</p>	<p>E-mail a children's author</p> <p>E-mail Museums and Galleries</p>
Publishing pupils' work on school and other websites.	<p>Pupil and parental consent should be sought prior to publication.</p> <p>Pupils' full names and other personal information should be omitted.</p>	<p>School website</p>
Publishing images including photographs of pupils.	<p>Parental consent for publication of photographs should be sought.</p> <p>Photographs should not enable individual pupils to be identified.</p> <p>File names should not refer to the pupil by name.</p>	<p>School website</p>
Communicating ideas within chat rooms or online forums.	<p>Only selected chat rooms dedicated to educational use and that are monitored directly by an adult should be used.</p> <p>Access to other social networking sites should be blocked. Pupils should never give out personal information.</p>	<p>With adult approval</p>
Audio and video conferencing to gather information and share pupils' work.	<p>Pupils should be supervised.</p> <p>Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.</p>	

Be Smart on the internet

S SAFE Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

M MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

A ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R RELIABLE Information you find on the internet may not be true, or someone online may be lying about who they are.

t TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

www.kidsmart.org.uk

KidSMART Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Childnet International
www.childnet.com

THINK U KNOW

Childnet.org.uk

Appendix 3:

The Avenue Primary Staff and Governor

Technology Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head Teacher.

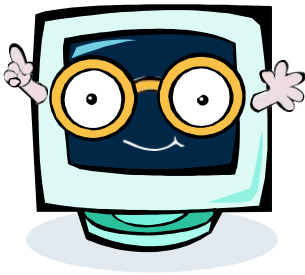
- I will only use the school’s hardware / email / Internet and any related technologies for professional purposes or for uses deemed ‘reasonable’ by the Head or Governing Body.
- All information transferred to and from school will be encrypted.
- I will not use my mobile phone in school apart from in the designated areas – staffroom or outside of the school day when no children are present.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications are compatible with my professional role.
- I will not contact pupils using email or phone (mobile or land line). Parents will not be contacted by personal mobile phone unless urgent contact is required and for school business, e.g. an emergency with their child on a school trip.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system for any school business.
- I will ensure that personal data (such as data held on MIS (Sims) software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any hardware or software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory, and will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- Images of pupils and or staff will only be taken, stored and used for professional purposes in line with school policy and with the consent of the parent/carer. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Head Teacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Head Teacher. I will respect copyright and intellectual property rights.
- I will support and promote the school’s e-Safety (including data security) policy and help pupils to be safe and responsible in their use of ICT and related technologies.

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature Date

Full Name(printed)

Appendix 4: Internet use - Rules for Responsible Internet Access



The Avenue Primary School

SMART Rules for Responsible Use of Technology

**The school has installed computers and Internet access to help our learning.
These rules will keep everyone safe and help us to be fair to others.**

I will only use school computers for school work.

I will only use the internet when my teacher has given me permission.

I will always be polite when using the internet or email.

I will not download files or bring in disks or USB memory sticks from outside the school unless I have been given permission.

I will NEVER give out my address or telephone number to any other internet user.

I will only send email that my teacher has approved so that they can be sure I am kept safe.

If I am uncomfortable or upset by anything I discover on the internet, I will report it to an adult immediately.

I will only use search engines that my teacher has approved.

I understand how old I have to be to use social media such as Facebook.

I understand that if I fail to keep these rules, I will not be allowed to use the internet in school.

The Avenue Primary School

Acceptable use and inclusion of children's work and photographs on the school web site or Twitter account.

Consent form

Please complete, sign and return to your child's teacher as soon as possible. Thank you for your co-operation.

Child's name:

Class:

Pupil Agreement.

I have seen and had explained our school's Acceptable Internet Use Policy rules. I understand that these rules are to protect me and other users of the school's computers and the Internet. I agree to follow these rules.

Signed:

Date:

Parent/Guardian's consent for Internet use.

I have read and understood the school's Acceptable Internet Use Policy and give permission for my child to access the Internet. I understand that the school will use a combination of filtering and supervision to ensure that pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature and content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:

Date:

Parent/Guardian's consent for publication of work and photographs on the school's web site.

I agree that, if selected, my child's work may form part of the school web site.

I also agree that photographs that include my child may be added to the site. I understand that such photographs will be of general school activities rather than of individual children. Children's full names will not be used on photographs but may be used on examples of their work.

Signed:

Date:

Setting up parental controls.

Besides checking PEGI ratings to help choose suitable games, parents can activate parental controls. This is much easier than it sounds and links to instructions can be found on our school website 'Parents' pages for many of the latest generation of game consoles - including Xbox 360, Wii U™, Sony Playstation 3 and PSP, Apple and PC controls.

Using these controls, you can restrict the rating or level of content that your child can play, and in some cases who your child plays with online and for how much time.

Parental controls ensure that your child has a fun and secure gaming experience.

Making sure your child's video game experience is safe and secure.

At The Avenue Primary School, we ensure that the children know how to keep themselves safe online and what to do if they feel uncomfortable about any content they might see.

The children also learn how to behave responsibly online both at home and at school in order to make everyone's online and gaming experience a good one.

We follow the SMART rules, which can be found on our school website.



The Avenue Primary School



Parents' Guide to Video and Online Safety.

A guide for parents about choosing age appropriate games, setting up parental controls, and making sure your child's video game experience is safe and secure.

Video games are a great source of learning and entertainment, but it is important for parents to appreciate what playing games today involves in order to keep their children safe.

A large number of games can be played over an internet connection. Being aware of the tools at a parent's disposal are crucial to ensure that children are safeguarded from inappropriate content and encounters with other players.



Some widely available video games contain graphic violence, virtual sex, violent and gory scenes, partial or full nudity, drug use, portrayal of criminal behaviour or other provocative and sensitive material.

Online gaming platforms often offer text chat, the use of headsets or even video for live communication with other players. Unfortunately, the anonymity of online gaming seems to encourage some players to post obscenities and unsuitable material which are difficult to control.

A Parents' and Carers' Guide to Video Game Ratings

It is probably true that most parents have grown up with the video or DVD classification system. However, this is not always the case with video games. All too often, the child is more adept at using the computer or games consoles and parents do not know how to access what he or she is playing. As a result, it is important to have something to guide parents when making a decision about whether a game is suitable or not.

The PEGI System (Pan-European Game Information)



From the summer of 2012, the PEGI system has been used by UK law for age rating video games. The age ratings 12, 16 and 18 are mandatory and it is illegal for a retailer to supply any game to someone below the age specified.

It is important to note that the age ratings relate to the content of the game and not how difficult it is to play. So, for example, a chess game would be too difficult to give to a 3 year old but it will have a '3' rating as the content is inoffensive. Likewise, a game which is easy enough for a 10 year old to play will be given an '18' rating if the subject matter or content is only suitable for adults. Therefore, a '3' or '7' rating does not mean that the game will be too easy for your child but that the content is suitable for primary age children.

Descriptors shown on the back of the packaging indicate the main reasons why a game has received a particular age rating. There are eight descriptors: violence, bad language, fear, drugs, sexual, discrimination, gambling and online gameplay with other people.

*Further information on the PEGI ratings can be found at :
<http://www.pegi.info/en/index/df33f>*