



West End Primary School

Ridge Terrace, Bedlington

Northumberland, NE22 6EB

Tel: 01670 822328

e-mail: admin@westend.northumberland.sch.uk

ICT and Computing Acceptable Use Policy for Pupils

2024 - 25

Approved by:	Headteacher
Date of Review:	Autumn 2024
Date of Approval:	Autumn 2024
Date of Next Review	Autumn 2025

Bedlington West End Primary School

ICT and Computing Acceptable Use Policy For Pupils

This policy is intended to be read and agreed in conjunction with the following policies:

- E-Safety
- Child Protection
- Anti-bullying
- Anti-racism
- Data protection

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times. This policy outlines our purpose in providing access to the Internet, e-mail and other communication technologies at Bedlington West End Primary School and explains how the school is seeking to avoid the potential problems that unrestricted access could create.

Internet Access in School

- All staff and any other adults involved in supervising children accessing the Internet, will be provided with the school ICT Acceptable Use Policy, and will have its importance explained to them.
- Our school ICT Acceptable Use Policy for Pupils is available for parents on the school website. Using the Internet to Enhance Learning Access to the Internet is a planned part of the curriculum that will enrich and extend learning activities and is integrated into schemes of work. As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for Internet use. Different ways of accessing information from the Internet will be used depending upon the nature of the material being accessed and the age of the pupils:
- access to the Internet may be by teacher demonstration
- pupils may be given a suitable web site to access using a link from their year group links page on the school website or by clicking on a link in a teacher-prepared Word document
- pupils may be provided with lists of relevant and suitable web sites which they may access
- older pupils may be allowed to undertake their own Internet search having agreed a search plan with their teacher; pupils will be expected to observe the Rules of Responsible Internet Use and will be informed that checks can and will be made on files and the sites they access.

Pupils accessing the Internet will be supervised by an adult, normally their teacher, at all times. They will only be allowed to use the Internet once they have been taught the Rules of Responsible Internet Use and the reasons for these rules. Teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor the children using the Internet.

Using Information from the Internet

In order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it:

- pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on television
- teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the Internet (as a non-moderated medium)
- when copying materials from the Web, pupils will be taught to observe copyright;
- pupils will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed.

Using E-mail

Email is to be solely used for educational purposes within school. Pupils are not permitted to send emails to each other or to staff outside of school hours. Email accounts will be supervised by the lead for Computing.

Maintaining the Security of the School ICT Network

Connection to the Internet significantly increases the risk that a computer or a computer network may be compromised or accessed by unauthorised persons. The ICT co-ordinator will update virus protection regularly, will keep up-to-date with ICT developments and work with the LEA as Internet Service Provider to ensure system security strategies to protect the integrity of the network are reviewed regularly and improved as and when necessary. Users should not expect that files stored on servers or storage media are always private.

Ensuring Internet Access is Appropriate and Safe

The Internet is freely available to any person wishing to send e-mail or publish a web site. In common with other media such as magazines, books and video, some material available on the Internet is unsuitable for pupils. Pupils in school are unlikely to see inappropriate content in books due to selection by publisher and teacher and the school will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the Internet. The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- our Internet access is purchased from Northumberland County Council which provides a service designed for pupils including a filtering system intended to prevent access to material inappropriate for children;

- our Rules for Responsible Internet Use are signed by parents and children each year;
- * Pupils have their own username and password which must be used to access the internet.
- children using the Internet will normally be working during lesson time and will be supervised by an adult (usually the class teacher) at all times;
- staff will check that the sites pre-selected for pupil use are appropriate to the age of the pupils;
- staff will be particularly vigilant when pupils are undertaking their own search and will check that the children are following the agreed search plan;
- pupils will be taught to use e-mail and the Internet responsibly in order to reduce the risk to themselves and others;
- the ICT co-ordinator will monitor the effectiveness of Internet access strategies;
- the ICT co-ordinator will ensure that occasional checks are made on files to monitor compliance with the school's ICT Acceptable Use Policy; 3
- the headteacher will ensure that the policy is implemented effectively;
- Internet searches are screened by SENSO Cloud and a report provided to the headteacher /deputy headteacher on a weekly basis, who can then monitor searches from each device based on this information.
- methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in accordance with national guidance and that provided by the LEA.

See Appendix 2 for pupil's permission status.

Generally, the above measures have been highly effective. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. Neither the school nor Northumberland County Council can accept liability for the material accessed, or any consequences of this.

A most important element of our Rules of Responsible Internet Use is that pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable. If there is an incident in which a pupil is exposed to offensive or upsetting material, responsibility for handling incidents involving children will be taken by the IT Co-ordinator and the Child Protection Officer in consultation with the Head Teacher and the pupil's class teacher.

All the teaching staff will be made aware of the incident if appropriate.

- If one or more pupils discover (view) inappropriate material our first priority will be to give them appropriate support. The pupil's parents/carers will be informed and given an explanation of the course of action the school has taken. The school aims to work with parents/carers and pupils to resolve any issue.
- If staff or pupils discover unsuitable sites the IT co-ordinator will be informed. The IT co-ordinator will report the URL and content to the ISP and the LEA; if it is thought that the material is illegal, after consultation with the ISP and LEA, the site will be referred to the relevant authorities.

Pupils are expected to play their part in reducing the risk of viewing inappropriate material by obeying the Rules of Responsible Internet Use that have been designed to help protect them from exposure to Internet sites carrying offensive material. If pupils abuse the privileges of access to the Internet or use of e-mail facilities by failing to follow the rules they have been taught or failing to follow the agreed search plan when undertaking their own Internet search, then sanctions consistent with our School Behaviour Policy will be applied. This will involve informing the parents/carers. Access to the Internet may also be denied for a period.

Photographs

Prior permission is sought from all parents regarding the use of images for printed publications, media, website and videos. Staff should check the relevant year group permission list before using images of children.

School Website and Facebook

Our school website and social media page on Facebook is intended to:

- provide accurate, up-to-date information about our school
- enable pupils' achievements to be published for a wide audience including pupils, parents, staff, governors, members of the local community and others
- promote the school.

All classes may provide items for publication on the school website. Class teachers will be responsible for ensuring that the content of the pupils' work is accurate, the quality of presentation is maintained and that photo permission forms are checked before submitting items for publication. All material must be the author's own work, crediting other work included and stating clearly that author's identity and/or status. The class teacher is responsible for uploading pages to the school website and the lad for computing along with the head teacher will ensure that the links work and are up-to-date, and that the site meets legal requirements.

The point of contact on the website will be the school address and telephone number. We do not publish pupils' full names or identify individuals on our web pages. Home information or individual e-mail identities will not be published.

Internet access and home/school links

Parents will be informed that pupils are provided with supervised Internet access as part of their lessons. We will keep parents in touch with future ICT developments both on the website and by newsletter. Pupils have permission to use their passwords for Mathletics, Spellodrome and School 360 at home, in order to support their learning outside of the classroom.

Cyberbullying

Cyberbullying can be defined as the use of Information and Communications Technology (ICT) deliberately to upset someone else and may involve email, virtual learning environments, chat rooms, social

networking sites, mobile and landline telephones, digital camera images and game and virtual world sites. Through Computing lessons, assemblies and PSHE, children will be taught the SMART rules:

SAFE - Keep safe by being careful not to give out personal information online.

MEETING - Never agree to meet anyone that you chat to on the internet; they may not be who you think they are. You can't be sure who you're talking to on the Internet.

ACCEPTING - Do not accept unusual e-mails. They may be trying to tempt you into opening them. They could contain viruses that can damage your computer. If this happens to you, tell an adult.

RELIABLE - Information on the internet may not be true – anyone can upload material to the internet. Always double check any information on a more reliable website.

TELL - If anything makes you feel worried tell your parents, teachers or an adult that you trust. They can help you to report it to the right place Or call a helpline like ChildLine on 0800 1111 in confidence.

Implementation and review process

This policy was reviewed as part of the E-safety policy agreed by the Strategic Direction Committee of the Governing Body and implemented in * 2018.

AUP agreement statements were created as an Appendix of the E-safety Policy and will be reviewed with the policy on a bi-annual basis or as required by changes in safeguarding responsibilities.

Date of next review: Autumn 2024

Appendix 2

	Staff & other adults				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Communication Technologies								
Mobile phones may be brought to school	*						*	
Use of mobile phones in lessons				*				*
Use of mobile phones in social time		*						*
Bluetooth enabled				*				*
Taking photos on mobile phones				*				*
Taking photos on digital cameras	*						*	
Use of personal hand held devices eg PDAs, PSPs		*						*
Use of personal email addresses in school, or on school network				*				*
Use of school email for personal emails				*				*
Use of chat rooms / facilities				*				*
Use of instant messaging				*				*
Use of social networking sites			*					*
Use of blogs		*					*	

User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					*
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					*
	adult material that potentially breaches the Obscene Publications Act in the UK					*
	criminally racist material in UK					*
	pornography				*	
	promotion of any kind of discrimination				*	
	promotion of racial or religious hatred				*	
	threatening behaviour, including promotion of physical violence or mental harm				*	
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				*		
Using school systems to run a private business				*		
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by NCC and the school				*		
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				*		
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				*		
Creating or propagating computer viruses or other harmful files				*		
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				*		
On-line gaming (educational)		*				
On-line gaming (non educational)		*				
On-line gambling				*		
On-line shopping / commerce		*				
File sharing		*				
Use of social networking sites		*				
Use of video broadcasting eg Youtube		*				