

St. Bede's Primary School e-Safety Policy



Aim

This policy sets out the ways in which St. Bede's Primary School, Jarrow will:

- educate all members of the school community on their rights and responsibilities with the use of technology;
- build both an infrastructure and culture of e-safety;
- work to empower the school community to use the Internet as an essential tool for lifelong learning.

Scope of Policy

This policy applies to all members of the school community, including staff, pupils, volunteers, parents/carers, visitors and community users.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying, which may take place out of school, but are linked to membership of the school.

The school will manage e-safety as described within this policy and associated behaviour and anti-bullying policies, and will inform parents and carers of known incidents of inappropriate e-safety behaviour that take place in and out of school.

Schedule for Development, Monitoring and Review

The Implementation of the e-safety policy will be monitored by an e-safety working group, meeting termly and reporting to the Governors annually.

The impact of the policy will be monitored by the e-safety working group by looking at:

- The log of reported incidents
- The Internet monitoring log
- Surveys or questionnaires of learners, staff, parents and carers
- Future developments

The e-safety policy will be reviewed annually and will be under continuous revision in response to significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.

Roles and responsibilities

The Headteacher is responsible for ensuring the safety (including e-safety) of all members of the school community.

The e-safety Leader will work with the Headteacher, who is also the designated Child Protection Coordinator, to have an overview of the serious child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate online contact with adults, potential or actual incidents of grooming and cyber-bullying.

An e-safety working group will work with the e-safety Leader to implement and monitor the e-safety policy and AUPs (Acceptable User Policies). This group is made up of e-safety Leader, Child Protection Coordinator, teacher linked to school council, link-governor, technician and pupils. Pupils are part of this group, working with them through the school council, to contribute their knowledge and use of technology. E-safety is an agenda item on each termly meeting of the school council.

Role	Responsibility
Governors	 Approve and review the effectiveness of the e-safety Policy.
	Delegate a governor to act as e-safety link.
	e-safety Governor works with the e-safety Leader to carry out regular
	monitoring and report to Governors.
Head	Ensure that all staff receive suitable CPD to carry out their e-safety
Teacher	roles.
and	Create a culture where staff and learners feel able to report incidents.
Senior	Ensure that there is a progressive e-safety curriculum in place.
Leaders	Ensure that there is a system in place for monitoring e-safety.
	Follow correct procedure in the event of a serious e-safety allegation
	being made against a member of staff or pupil.
	Inform the local authority about any serious e-safety issues.
	 Ensure that the school infrastructure/network is as safe and secure as possible.
	 Ensure that policies and procedures approved within this policy are implemented.
	Use an audit to annually review e-safety with the school's technical support
e-safety	Lead the e-safety working group.
Leader	 Log, manage and inform others of e-safety incidents and how they have been resolved where this is appropriate.
	• Lead the establishment and review of e-safety policies and documents.
	 Lead and monitor a progressive e-safety curriculum for pupils.
	 Ensure all staff are aware of the procedures outlined in policies relating to e-safety.
	Organise training and advice for staff.
	 Attend updates and liaise with the LA e-safety staff and technical staff.
	Meet with Senior Leadership Team and e-safety Governor to regularly discuss incidents and developments
	Coordinate work with the school's designated Child Protection Coordinator

Teaching Participate in any training and awareness raising sessions. Read, understand and sign the Staff AUP. and Act in accordance with the AUP and e-safety Policy. **Support** Report any suspected misuse or concerns to the e-safety Leader and Staff check this has been recorded. Provide appropriate e-safety learning opportunities as part of a progressive e-safety curriculum and respond. Model the safe use of technology. Monitor ICT activity in lessons, extra-curricular and extended school activities. Demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with school ethos and policies, including at the time of a Critical Incident Read, understand and sign the Pupil AUP and the agreed class Internet **Pupils** rules. Participate in e-safety activities, follow the AUP and report concerns for themselves or others. Understand that the e-safety Policy covers actions out of school that are related to their membership of the school **Parents** Endorse (by signature) the Pupil AUP. Discuss e-safety issues with their child(ren) and monitor their home and use of technology (including tablets, mobile phones and games devices) Carers and the Internet. Access the school website in accordance with the relevant school AUP. Keep up to date with issues through newsletters and other opportunities. Inform the Headteacher of any e-safety issues that relate to the Maintain responsible standards when using social media to discuss school issues. **Technical** Ensure the school's ICT infrastructure is as secure as possible and is Support protected from misuse or malicious attack. Provider Ensure users may only access the school network through an enforced password protection policy. Maintain and inform the Senior Leadership Team of issues relating to filtering. Keep up to date with e-safety technical information and update others as relevant. Ensure use of the network is regularly monitored in order that any misuse can be reported to the e-safety Leader for investigation. Ensure monitoring systems are implemented and updated. Ensure all security updates are applied. Sign an extension to the Staff AUP detailing their extra responsibilities Sign and follow the Guest/Staff AUP before being provided with Community access to school systems. Users

Education of Pupils

Pupils to 'understand what constitutes unsafe situations and are highly aware of how to keep themselves and others safe in different situations including in relation to e-safety'

School Inspection Handbook - Ofsted 2014

A progressive planned e-safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited. Breadth and progression is ensured through implementation of the 2014 Somerset Byte awards and the e-safety progression which is part of the adapted Somerset Primary Computing

Within this:

Curriculum that we follow at St. Bede's.

- Key e-safety messages are reinforced through discrete e-safety lessons, along with Safer Internet Day (February), Cool to be Kind Week (Anti-Bullying Week in November) and throughout other lessons, where appropriate.
- Pupils are taught to keep themselves safe online and to be responsible in their use of different technologies as detailed in our scheme of work.
- Pupils are guided to use age appropriate search engines for research activities. Staff
 are vigilant in monitoring the content of the websites visited and encourage pupils to
 use specific search terms to reduce the likelihood of coming across unsuitable
 material.
- In lessons where Internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Pupils are taught to be critically aware of the content they access online and are guided to validate the accuracy and reliability of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Pupils are taught about current issues such as online gaming and obsessive use of technology.
- Pupils will sign an AUP for their class at the beginning of each school year.
- Pupils are educated to recognise and respond appropriately to different forms of bullying, including cyber-bullying.

Education and information for parents and carers

Parents and carers will be informed about the ways the Internet and technology is used in school. They have a critical role to play in supporting their children with managing e-safety risks at home, reinforcing key messages about e-safety and regulating their home experiences. The school supports parents and carers to do this by:

- Providing clear AUP guidance, which they are asked to sign with their children, and website updates;
- Raising awareness through activities such as Safer Internet Day or other meetings, as appropriate;
- Providing and maintaining links to up to date information on the school website.

Training of Staff and Governors

There is a planned programme of e-safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this and the AUPs. This includes:

- An annual audit of the e-safety training needs of all staff.
- All new staff receiving e-safety training as part of their induction programme.
- Providing information to supply and student teachers on the school's e-safety procedures.
- The e-safety Leader receiving LA training sessions and by reviewing regular e-safety updates from the LA.
- This e-safety Policy and its updates being shared and discussed in staff meetings and in Governor meetings.
- The e-safety Leader providing guidance and training as required to individuals and seeking LA support on issues.
- Staff and governors are made aware of the UK Safer Internet Centre helpline 0844 381 4772

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.

The school will follow procedures in place to support anyone in the school community affected by cyberbullying.

Pupils and staff are made aware of a range of ways of reporting concerns about cyberbullying e.g. telling a trusted adult, Childline Phone number 0800 1111.

Pupils, staff and parents and carers will be encouraged to report any incidents of cyberbullying and advised to keep electronic evidence.

All incidents of cyberbullying reported to the school will be recorded by the school.

The school will follow procedures to investigate incidents or allegations of cyberbullying.

The school will take steps, where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.

Pupils, staff and parents and carers will be required to work with our school to support the approach to cyberbullying and our school's e-safety ethos.

Sanctions for those involved in cyberbullying will follow those for other bullying incidents and may include:

- the bully being asked to remove any material deemed to be inappropriate or the service provider being contacted to remove content if the bully refuses or is unable to delete content.
- Internet access being suspended at the school for a period of time. Other sanctions
 for pupils and staff may also be used in accordance to the schools anti-bullying,
 behaviour policy or AUP.
- the parent and carers of pupils being informed.
- the police being contacted if a criminal offence is suspected.

Technical Infrastructure

The person responsible for the school's technical support and will sign a technician's AUP, in addition to the staff AUP.

The school ensures, when working with our technical support provider, that the following quidelines are adhered to:

- The School ICT systems are managed in ways that ensure that the school meets esafety technical requirements
- There are regular reviews and audits of the safety and security of school ICT systems.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations and other devices from accidental or malicious attempts which might threaten the security of the school systems and data with regard to:
 - o The downloading of executable files by users.
 - The extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices used out of school.
 - The installation of programs on school devices unless permission is given by the technical support provider or Computing/ICT coordinator.
 - o The use of removable media (e.g. memory sticks) by users on school devices.
 - The installation of up-to-date virus software.

- Access to the school network and Internet will be controlled with regard to:
 - users having clearly defined access rights to school ICT systems through group policies.
 - users (apart from Foundation Stage and Key Stage One pupils) being provided with a username and password.
 - users being made aware that they are responsible for the security of their username and password and that they must not allow other users to access the systems using their log-on details.
 - users must immediately report any suspicion or evidence that there has been a breach of security.
 - o an agreed process being in place for the provision of temporary access of "guests" (e.g. trainee or supply teachers, visitors) onto the school system. All "guests" must sign the staff AUP and are made aware of this e-safety policy
 - Key Stage 1 pupils' access will be supervised with access to specific and approved online materials
 - Key Stage 2 pupils' will be supervised. Pupils will use age-appropriate search engines and online tools and activities
- The Internet feed will be controlled with regard to:
 - The school maintaining a managed filtering service provided by an educational provider.
 - o The school monitoring Internet use.
 - Requests from staff for sites to be removed from the filtered list being approved by the Senior Leadership Team and logged onto the Open Zone Help Desk by the Computing Coordinator/ E-Safety Leader.
 - o Filtering issues being reported immediately.
- The IT System of the school will be monitored with regard to:
 - The school IT technical support regularly monitoring and recording the activity of users on the school IT systems.
 - E-safety incidents being documented and reported immediately to the e-safety Leader who will arrange for these to be dealt with immediately, in accordance with the AUP.

Data Protection

The school's Data Protection Policy provides full details of the requirements that need to be met in relation to the Data Protection Act 1998.

The School will:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- use personal data only on secure password protected computers and other devices.
- ensure that users are properly 'logged-off' at the end of any session in which they are accessing personal data.
- store or transfer data using approved services such as remote access, the South Tyneside Learning Platform, encryption and secure password protected devices.
- make sure data is deleted from the device, once it has been transferred or its use is complete.

Use of digital and video images

Photographs and video taken within school are used to support learning experiences across the curriculum, to share learning with parents and carers on our school's learning platform and to provide information about the school on the website. The school will:

- when using digital images, instruct staff to educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images, including on social networking sites.
- allow staff to take images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.
- make sure that images or videos that include pupils will be selected carefully with their knowledge.
- seek permission from parents or carers (when child joins our school) before images or videos of pupils are electronically published.
- all parties must recognise that any published image could be reused and repurposed
- ensure that pupils' full names will not be used anywhere on the school website, particularly in association with photographs.
- not publish pupils' work without their permission and the permission of their parents
- keep the written consent where pupils' images are used for publicity purposes, until the image is no longer in use.
- store photographs in a protected storage area of the school server, from where they will be permanently deleted after use.

Communication

A wide range of communications technologies have the potential to enhance learning. The school will:

With respect to e-mail:

- ensure that the school uses a secure business email system for communication
- ensure that personal information is not sent via unsecure email
- ensure that governors use a secure e-mail system
- ensure that any digital communication between staff and pupils or parents and carers is professional in tone and content
- make users aware that email communications will be monitored by the school
- inform users what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature
- provide pupils at Key Stage 2 with a monitored, individual, educational school e-mail addresses
- teach pupils about email safety issues through the scheme of work and implementation of the AUP
- only publish official staff email addresses where this required

With respect to social media e.g. YouTube, Facebook, Twitter, blogging and personal publishing:

- Discuss with staff the personal use of email, social networking, social media and personal publishing sites as part of staff induction, building an understanding of safe and professional behaviour in line with Teaching Standards 2012
- Staff are advised that no reference should be made to pupils, parents/carers or school staff.
- Advise all members of the school community not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory
- Register concerns (e.g. recording in e-safety log) regarding pupils' inappropriate use
 of email, social networking, social media and personal publishing sites (in or out of
 school) and raise with their parents and carers, particularly when concerning pupils'
 underage use of sites.
- Support staff in dealing with the consequences of hurtful or defamatory posts about them online.

With respect to mobile phones:

- Inform staff that personal mobile phones should only be used at break, lunchtimes and in restricted areas when they are not in contact with pupils', unless they have the permission of the Headteacher
- Inform staff that they are not allowed to use personal devices to take photographs or video in school for any purpose.
- Advise staff not to use their personal mobile phone to contact pupils, parents and carers
- Provide the school mobile phone for activities that require them (e.g. Educational visits)
- Inform visitors of the school's expectations regarding the use of mobile phones
- Inform pupils that they are not allowed to bring mobile phones into school.
- Maintain the right to collect and examine any phone that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on the school Internet connection.

The following table shows how the school considers the way these methods of communication should be used:

	Staff & other adults			Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selecte staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/presence	Not allowed
Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones/personal devices				✓				✓
Taking photos on school devices (parental permission obtained)	✓						✓	
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 social networking sites				✓				✓
Use of Twitter				✓				✓
Use of video broadcasting eg Youtube				✓				✓

Assessment of Risk

Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances the school will examine and adjust the e-safety Policy. Part of this consideration will include a risk assessment:

- looking at the educational benefit of the technology
- considering whether the technology has access to inappropriate material

However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor South Tyneside Council can accept liability for the material accessed, or any consequences resulting from Internet use.

All users need to be reminded that the use of computer systems, without permission or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Police.

Reporting and Response to Incidents

The school will follow South Tyneside's flowcharts to respond to illegal and inappropriate incidents. The Headteacher and e-safety leader will be involved in this process and the same designated computer will be used for the duration of any investigation. All sites and content checked will be recorded and screen shots, signed and dated, will be kept where this is appropriate. Should content being reviewed include images of Child abuse then the monitoring will be halted and referred to the Police immediately.

- All members of the school community will be informed about the procedure for reporting esafety concerns (such as breaches of filtering, cyberbullying, illegal content)
- The Headteacher will record all reported incidents and actions taken in the School e-safety incident log.
- The Child Protection Coordinator will be informed of any e-safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures.
- The school will manage e-safety incidents in accordance with the School Behaviour Policy, where appropriate
- The school will inform parents and carers of any incidents or concerns in accordance with school procedures
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact SouthTyneside's Safeguarding Team and escalate the concern to the police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding for Schools Adviser, Local Authority Designated Officer (LADO) or Senior Education Technology Adviser

If an incident or concern needs to be passed beyond the school then the concern will be escalated to the Safer Communities Officer.

Should serious e-safety incidents take place, the following external persons and agencies should be informed: Safer Communities Officer: Graeme Littlewood: Tel: 4247935

Senior Education Technology Adviser M.Hamilton, OpenZone.Tel: 4246330

Local Authority Designated Officer (LADO) Jean Hughes: Tel: 4247747

Northumbria Police

The police will be informed where users 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, 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, verbally abusive or threatening material information which is false and known or believed by the sender to be false.

Sanctions and Disciplinary proceedings

Sanctions and disciplinary procedures may be taken where users 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
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- pornography, adult or mature content
- promotion of any kind of discrimination, racial or religious hatred
- personal gambling or betting
- personal use of auction sites
- any site engaging in or encouraging illegal activity
- 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 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 (e.g. financial or personal information, databases, computer or network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the Internet.

Sanctions for Misuse:

Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity.

Handling Infringements

Whenever a student or staff member infringes the E-Safety Policy, the final decision on the level of sanction will be at the discretion of the Headteacher or the Governors in the case of the Headteacher.

The following are provided as exemplification only:

Pupils:

Category A infringements:

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends.
- Use of unauthorised instant messaging / social networking sites

Category A Sanctions:

Referred to e-safety leader.

Referred to Headteacher.if deemed serious or child protection issue

Category B infringements:

- Continued use of non-educational sites during lessons after being warned.
- Continued unauthorised use of email after being warned. Continued unauthorised use of mobile phone (or other new technologies) after being warned.
- Continued use of unauthorised sites such as instant messaging / chat rooms, social networking sites.
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

Category B Sanctions:

- Referred to E-Safety Leader/Headteacher Next steps/consequences agreed.
- Parents informed.

Category C infringements:

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Transmission of commercial or advertising material

Category C Sanctions:

- Referred E-Safety Leader/Headteacher. Next steps/consequences agreed by both.
- Parents informed.
- Removal of Internet and/or Learning Platform access rights for a period.
- Removal of equipment if applicable.

If inappropriate web material is accessed:

- Ensure appropriate technical support filters the site.
- Inform LA as appropriate.

Category D infringements:

- Continued sending of emails regarded as harassment or of a bullying nature after being warned.
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

Category D Sanctions:

- Referred to e-safety leader/Headteacher. Next steps/consequences agreed by both.
- Parents informed.
- Removal of Internet and/or Learning Platform access rights for a period.
- Removal of equipment if applicable.
- Refer to LA E-Safety officer and/or Community Police Officer.

Other safeguarding actions:

- 1. Secure and preserve any evidence
- 2. Inform the sender's e-mail service provider

Staff

Category A infringements (Misconduct):

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network

Category A Sanctions:

- Referred to Line Manager and E-Safety leader.
- If deemed more serious, referred to Headteacher and warning given.

Category B infringements (Gross Misconduct):

- Serious misuse of, or deliberate damage to, any school computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;

- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

Category B Sanctions:

- Referred to Headteacher.
- Governors informed /follow school disciplinary procedures.
- Report to LA Personnel/Human Resources.
- Report to Police, if appropriate.

Other safeguarding actions:

- 1. Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- 2. Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
- 3. Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that, the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken. Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority.

In the case of **Child Pornography** being found, the member of staff should be **immediately** suspended and the Police should be contacted.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

In addition, the following indicates school policy on these uses of the Internet:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable
Online games (educational)	✓			
Online gaming (non-educational)				✓
Online gambling				✓
Online shopping / commerce			✓	

E-Safety Policy					
Date approved by Governing Body:					
Signature of Chair of Governors:					
Next Review Date:	Autumn Term 2019				