Bozeat Community Primary School & Nursery

Online Safety Policy

Approved by:	Full Governing Body	**Date:** 21st May 2021
Last reviewed on:	19th May 2021	
Next review due by:	May 2022	

Information and Communication Technology

Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Downloading from the internet
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

At Bozeat Community Primary School, we understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Online Safety Policy

Our Online Safety policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all technologies to safeguard all adults and children within school. The policy recognises the ever-changing nature of emerging technologies and highlights the need for regular review to incorporate development within ICT.

E-safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Anti-Bullying, Data Protection, and our Curriculum statement.

1. Purpose

The use of the internet as a tool to develop learning and understanding has become an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children access these technologies.

The risks include:

- Commercial issues with spam and other inappropriate e-mail.
- Grooming by predators, usually pretending to be someone younger than their true age.
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or any mobile device.
- Malware - Worms, **viruses**, trojans, backdoors, and ransomware.
- Sexting-the sending of indecent personal images, videos or text via mobile phones for private viewing. Can potentially be widely distributed and publicly viewed.

- On-line content which is abusive or pornographic.

- It is also important that adults are clear about the procedures, for example, only contacting children and young people about homework via a school e-mail address, not a personal one, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

- Online Bullying/Cyber-bullying - bullying virtually as behaviour by an individual or group, repeated over time that is intended to hurt another individual or group either physically or emotionally.

2. Roles and responsibilities of the school

a. Governors and Head of School

It is the overall responsibility of the Head of School with the Governors to ensure that there is an overview of online safety (as part of the wider remit of Child Protection) across the school with further responsibilities as follows:

1. The Head of School has designated an Online safety Leader to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-safety is addressed in order to establish a safe ICT learning environment. All staff and students are aware of who holds this post within the school.

2. Time and resources should be provided for the online safety Leader and staff to be trained and update policies, where appropriate.

3. The Head of School is responsible for promoting e-safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.

4. The Head of School should inform the Governors at the standards and school improvement committee meetings about the progress of or any updates to the safety curriculum (via PSHE or ICT) and ensure Governors know how this relates to child protection.

5. At the Full Governor meetings, all Governors are to be made aware of e-safety developments from the standards and school improvement committee meetings.

6. The Governors MUST ensure Child Protection is covered with an awareness of safety and how it is being addressed within the school, as it is the responsibility of Governors to ensure that all Child Protection guidance and practices are embedded.

7. An e-safety Governor (can be the ICT or Child Protection Governor) ought to challenge the school about having an e – safety policy with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT, including:

Challenging the school about having:

- Firewalls,
- Anti-virus and anti-spyware software,
- Filters,
- Using an accredited ISP (Internet Service Provider),
- Awareness of wireless technology issues,
- A clear policy on using personal devices,
- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures of the school.

b. Online safety Leader

It is the role of the designated e-safety Leader to:

1. Appreciate the importance of e-safety within school and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.

2. Establish and maintain a safe ICT learning environment within the school.

3. Ensure that the Online safety policy is reviewed annually, with up-to-date information available for all staff to teach e-safety and for parents to feel informed and know where to go for advice.

4. Ensure that filtering is set to the correct level for staff, children and young people, in the initial set up of a network, stand-a-lone PC, staff/children laptops and the learning platform or ensure the technician is informed and carries out work as directed.

5. Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.

6. Report issues as appropriate

7. Liaise with the PSHE, Designated Safeguarding Lead (DSL) and ICT leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.

8. Update staff training (all staff) according to new and emerging technologies so that the correct e-safety information can be taught or adhered to.

9. Transparent monitoring of the internet and on-line technologies – staff can access all pupil email accounts.

10. Home use of school or setting equipment must be in keeping with this policy.

11. Personal equipment may be used at school subject to appropriate electrical testing at work and used in keeping with this policy.

12. Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified.

13. Work alongside the ICT technician to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.

14. Ensure that staff can check for viruses on laptops, stand-a-lone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.

15. Ensure there is regular monitoring of internal e-mails, where:

- Blanket e-mails are discouraged.

- Tone of e-mails is in keeping with all other methods of communication.

- Report overuse of blanket e-mails or inappropriate tones to the Head of School and/or Governors.

c. Staff / Governors or other adults within the school

It is the responsibility of all adults within the school or other setting to:

1. Ensure that they know who the DSL is within school or other setting, so that any misuse or incidents can be reported which involve a child. Where an allegation is made against a member of staff it should be reported immediately to the Head of School. In the event of an allegation made against the Head of School, the Chair of Governors must be informed immediately.

2. Be familiar with the Behaviour, Anti-bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. In the event that a procedure is unknown, they will refer to the head of School immediately.

3. Check the filtering levels are appropriate for their children and young people and are set at the correct level. Report any concerns to the e-safety Leader.

4. Alert the e-safety Leader of any new or arising issues and risks that may need to be included within policies and procedures.

5. Ensure that children and young people are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner.

6. Children and young people should know what to do in the event of an incident.

7. Be up-to-date with e-safety knowledge that is appropriate for the age group and reinforce through the curriculum.
8. Sign an Acceptable Use Statement to show that they agree with and accept the rules for staff using non-personal equipment, within and beyond the school environment, as outlined in appendices (this will vary from school to school, but is advisable so that there is staff protection against allegations made by children and young people).

9. Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998.

10. Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
11. **School business managers** will need to ensure that they follow the correct procedures for any data required to be taken from the school premises (encryption software on any equipment taken off site).

12. Report accidental access to inappropriate materials to the e-safety Leader and learning platform helpdesk in order that inappropriate sites are added to the restricted list.

13. IT Technicians will be responsible for maintaining anti-virus software, and in liaison with the teachers, use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the internet on a regular basis, especially when not connected to the school/educational setting's network.

14. Report incidents of personally directed "bullying" or other inappropriate behaviour via the internet or other technologies using the NCC accident/incident reporting procedure in the same way as for other non-physical assaults.

d. Children and young people

1. Children and young people should be:

2. Involved in the review of Acceptable Use Rules through the school council or other appropriate group, in line with this policy being reviewed and updated.

3. Responsible for following the Acceptable Use Rules whilst within school as agreed at the beginning of each academic year or whenever a new child attends the school or setting for the first time.

4. Taught to use the internet in a safe and responsible manner through ICT, PSHE or other clubs and groups.

5. Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).

3. Appropriate and Inappropriate Use

a. Staff / Governors or other adults within the school

1. Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.

2. They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

3. All staff should receive a copy of the Acceptable Use Policy and a copy of the Acceptable Use Rules, which then need to be signed, returned to school or setting to keep under file with a signed copy returned to the member of staff.

4. The Acceptable Use Rules will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

5. When using school provided devices from home, the same Acceptable Use Rules will apply. The acceptable use should be similar for staff to that of the children and young people so that an example of good practice can be established. Please refer to acceptable use agreement for acceptable use rules.

In the event of inappropriate use

1. If a member the school who has signed the acceptable usage policy, is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Head of School immediately and then the Allegations Procedure (Section 12, LSCBN) and the Safeguarding Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

2. In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

b. By Children or Young People

Acceptable Use Rules and the letter for children, young people and parents/carers are signed when children start the school. These detail how children and young people are expected to use the internet and other technologies within school or other settings, including downloading or printing of any materials. The rules are there for children and young people to understand what is expected of their behaviour and attitude when using the internet which then enables them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so. The Rules will be displayed within the immersive classroom and on the school website.

Schools or educational settings should encourage parents/carers to support the rules with their child or young person. This can be shown by signing the Acceptable Use Rules together so that it is clear to the school or setting that the rules are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the internet beyond school.

Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File-sharing via e-mail and google drive for example, weblogs or any other means on-line should be appropriate and be copyright free when using the learning platform in or beyond school.

In the event of inappropriate use

Should a child or young person be found to misuse the on-line facilities whilst at school, or in a setting, the following consequences should occur:

1. The online safety lead will be alerted and informed

2. Any child found to be misusing the internet by not following the Acceptable Use Rules may have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.

3. Further misuse of the rules may result in not being allowed to access the internet for a period of time and another letter will be sent home to parents/carers.

4. A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

5. In the event that a child or young person accidentally accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window.

6. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they have been taught that they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice.
7. Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

5. Good Habits

Online safety depends on effective practice at a number of levels:

1. Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.

2. Sound implementation of an online safety policy in both administration and curriculum, including secure school network design and use.

3. Safe and secure broadband for learning including the effective management of content filtering.

4. National Education Network standards and specifications.

5. School online safety Policy.

6. The ICT Team will liaise with the DSL as the roles overlap to ensure e-safety procedures are in place.

7. Our online safety policy has been written by members of the SLT using the Government guidance. It has been agreed by all staff and approved by governors.

8. The online safety policy will be reviewed annually, or more frequently as required, to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.

6. Importance of Internet Usage

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access. The following concepts, skills and competencies should have been taught by the time they leave Year 6:

- Approaching information found online with 'critical eyes'
- Internet literacy.
- Making good judgements about websites and e-mails received.
- knowledge of risks such as viruses and opening mail from a stranger.
- Access to resources that outline how to be safe and responsible when using any online technologies.
- Knowledge of copyright and plagiarism issues.
- File-sharing and downloading illegal content.
- Uploading information – know what is safe to upload and not upload personal information.
- Where to go for advice and how to report abuse.
- A good understanding of what online bullying is and how to report bullying to trusted adults in school.

We use the www.thinkuknow.co.uk resources for KS1 and KS2, within ICT to teach responsible use of the internet, emails and keeping safe.

Teachers and pupils may use the internet outside school for personal and educational use.

In order to ensure their own safety and security it is essential they understand and abide by the school e-safety rules.

7. Pupils with additional learning needs

Bozeat Community Primary School recognises that some pupils are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss. The school or setting should strive to provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each pupil. When implementing an appropriate e-Safety policy and curriculum, Bozeat Community Primary School will seek input from specialist staff as appropriate, including the SENDCo and the Child in Care Designated Teacher. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of online safety awareness sessions and internet access

8. Filtering:

1. The school will work in partnership with the Local Authority and the Internet Service Provider to ensure filtering systems are as effective as possible.

2. The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.

3. If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the online safety coordinator or network manager, who will then ensure the ISP is informed immediately.

4. Social networking sites and newsgroups are blocked for pupil use via the filtering system.

9. Safety

a. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. Pupils will not access the internet without appropriate supervision.

b. Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.

c. Pupils will be advised never to give out personal details of any kind which may identify them or their location.

d. Pupils should be advised not to place personal photos on any social network space.

e. Pupils should be advised frequently on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

f. Mobile phones will not be used by pupils in school.

g. Children should use a search engine that is age appropriate.

h. If the children see something or search for something that is inappropriate they are taught how to deal with this…turn off the screen/minimise the screen and report to the adult in charge of the session. The adult then passes this information on to the online safety lead to log and take further with schools broadband as a filtering issue.

i. Pupils will be taught to view information gathered online with 'critical eyes'.

10. Mobile Phones

Staff/governors will not use personal mobile phones to take pictures or record video of any of the children. If photos or video are needed, whether it be on school premises or trips/visits, then school has digital cameras or tablets to use.

11. Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material (e.g. supervision/correct filtering levels). However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.

11 Teaching and Learning within Bozeat Community Primary School (BPS)

a. All current staff, governors and pupils are automatically granted Internet access.

b. All staff and governors must read and sign the 'staff code of conduct' before using any school ICT resource.

c. Parents will be informed that pupils will be provided with supervised Internet access.

d. Parents will be asked to sign and return a consent form for pupil access.

e. Pupils will be asked to sign internet and email rules with parents.

f. Internet access will be planned to enrich and extend learning activities.

g. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

h. School will ensure that the use of Internet derived materials by pupils and staff and governors complies with copyright law.

i. Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

12 Personal Use

1. It will be possible to access school website and learning links from home, but we would advise parental supervision and regular reminders to follow the safety guidelines as taught in school.

2. Published Content and the School Web Site

3. The contact details on the Web site should be the school address and telephone number. Staff or pupils personal information will not be published.

4. The Head of School or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

5. Children will not access personal accounts such as emails through school systems whilst using school equipment.

13. Publishing Pupils' Images and Work

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified, unless there is prior parental agreement.

Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.

Annual written permission from parents or carers will be obtained before photographs of pupils' and their work are published on the school Web site.

14. Information System Security

1. School ICT systems capacity and security will be reviewed regularly in discussion with the Local Authority and the ICT team at Wollaston as appropriate.

2. Virus protection will be installed and updated regularly.

3. Security strategies will be discussed with Wollaston and the Local Authority as appropriate.

15. Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the EU General Data Protection Regulation.

Handling online safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the Head of School.

- 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 as outlined in the school brochure.

- Discussions will be held with the Police to establish procedures for handling potentially illegal issues.

16. Social networking advice for staff and governors

Social networking outside of work hours, on non-school issue equipment, is the personal choice of all school staff/governors. Owing to the public nature of such websites, it is advisable for all to consider the possible implications of participation. The following advice should be considered if involved in social networking:

1. Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.

2. Staff should not engage in personal online contact with current students or past students outside of Head of School authorised systems (e.g. school email account for homework purposes).

3. Bozeat Community Primary School advise all staff members who are participating in social networking to activate the highest level of privacy settings possible on their profiles to prevent unsolicited contact by current and past children or parents.

4. Staff/ governors will ensure that their online activity, both in the school setting and outside, will not bring their professional role into disrepute.

5. Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.

6. Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students).

7. There is well documented evidence to suggest that social networking can be a highly effective tool for communicating with students on a professional level. Some schools and other educational settings have set up accounts on Facebook to manage and monitor public and pupil communications through designated members of staff. Other such professional social networking tools include EdModo or Virtual Learning Environments such as Moodle which contain similar features.

17. Communication of Policy

Pupils
Rules for Internet access will be posted in all networked rooms.

Pupils will be informed that Internet use will be monitored and should not be unsupervised.

Staff
All staff/governors have access to the School e-safety 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.

Parents
Parents' attention will be drawn to the School e-safety Policy in newsletters, the school brochure, school website and through the e-safety rules letter.