

# Burnhope Primary School **E-safety Policy**



Our E-safety Policy has been written by the school, building on the DCC e–Safety Policy and government guidance.

It has been agreed by the senior management and approved by governors.  
It will be reviewed annually.

Mrs Atwill is the school's e–Safety Coordinator.

Modified with grateful permission from Kent County Council

Policy Adopted by Governors – March 2021  
Policy to be reviewed by Governors – March 2022

## 1.2 Teaching and learning

### 1.2.1 Why is Internet use important?

- The rapid developments in electronic communications are having many effects on society. The Internet is a part of everyday life for education, business and social interaction.
- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- 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 functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

### 1.2.2 How does Internet use benefit education?

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with DCC and DfE;
- access to learning wherever and whenever convenient.

### 1.2.3 How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The school will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

### 1.2.4 How will pupils learn how to evaluate Internet content?

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to use search engines appropriately for their age.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

## 1.3 Managing Information Systems

### 1.3.1 How will information systems security be maintained?

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- The school will comply with the terms of the data protection act, and is responsible for registering with the information commissioner's office. [www.ico.gov.uk](http://www.ico.gov.uk) advice is available from [www.ico.gov.uk/for\\_organisations/sector\\_guides/education.aspx](http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx)
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

### 1.3.2 How will email be managed?

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.
- Schools will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- Staff should not use personal email accounts during school hours or for professional purposes.

### 1.3.3 How will published content be managed?

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

### 1.3.4 Can pupils' images or work be published?

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Pupils' work can only be published with their permission or that of their parents.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- Burnhope Primary School has a policy regarding the use of photographic images of children which outlines policies and procedures.

### 1.3.5 How will social networking, social media and personal publishing be managed?

- Children and staff will not be able to access social networking sites in school. Despite this, we are aware that children may access these sites at home.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites' terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Newsgroups will be blocked unless a specific use is approved.

- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

### 1.3.6 How will filtering be managed?

- The school's broadband access includes filtering.
- The school will have system in place to make changes to the filter, including deciding who is responsible for authorising changes.
- The school will work with DCC to review filtering
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Durham Police or CEOP

### 1.3.7 How will videoconferencing be managed?

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Videoconferencing contact information will not be put on the school Website.
- The equipment must be secure and if necessary locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.
- Responsibility for the use of the videoconferencing equipment outside school time will be established with care.

#### **Users**

- Pupils will ask permission from a teacher before making or answering a videoconference call.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parents' and carers' consent should be obtained prior to children taking part in videoconferences.
- Only key administrators should be given access to videoconferencing administration areas or remote control pages.

- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

### **Content**

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

### 1.3.8 How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use or Mobile Phone Policy.

### 1.3.9 How should personal data be protected?

The Data Protection Act 1998 (“the Act”) gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
  - Processed for specified purposes
  - Adequate, relevant and not excessive
  - Accurate and up-to-date
  - Held no longer than is necessary
  - Processed in line with individual's rights
  - Kept secure
  - Transferred only to other countries with suitable security measures.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

## 1.4 Policy Decisions

### 1.4.1 How will Internet access be authorised?

- All staff will read and sign the School Acceptable Use Policy before using any school ICT resources.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

### 1.4.2 How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate 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 DCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate.
- 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 the police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

### 1.4.3 How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents or concerns as and when required.
- 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 the Children’s Safeguard Team or e-Safety officer 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 Area Children’s Officer or the County e-Safety Officer.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer to communicate to other schools in Durham.

#### 1.4.4 How will e–Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the School’s complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children’s Safeguard Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school’s disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

#### 1.4.5 How is the Internet used across the community?

- The school will liaise with local organisations to establish a common approach to e–Safety.
- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.
- The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

#### 1.4.6 How will Cyberbullying be managed?

Cyberbullying can be defined as “The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone” DCSF 2007

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- Sanctions for those involved in cyberbullying may include:
  - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
  - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance with the schools anti-bullying, behaviour policy or Acceptable Use Policy.
  - Parent/carers of pupils will be informed.
  - The Police will be contacted if a criminal offence is suspected.

#### 1.4.7 How will Learning Platforms be managed?

- SLT and staff will regularly monitor the usage of the Durham Learning Gateway by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the DLG.
- Only members of the current pupil, parent/carers and staff community will have access to the DLG.
- All users will be mindful of copyright issues and will only upload appropriate content onto the DLG.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns about content on the DLG may be recorded and dealt with in the following ways:
  - a) The user will be asked to remove any material deemed to be inappropriate or offensive.
  - b) The material will be removed by the site administrator if the user does not comply.
  - c) Access to the DLG for the user may be suspended.
  - d) The user will need to discuss the issues with a member of SLT before reinstatement.
  - e) A pupil's parent/carer may be informed.
- A visitor may be invited onto the DLG by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

## 1.4.8 How will mobile phones and personal devices be managed?

- The use of mobile phones and other personal devices by students is not allowed and children will not bring these to school.
- The use of mobile phones and other personal devices by staff in school is covered in the school Acceptable Use or Mobile Phone Policy.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- If a pupil is found to have a mobile phone in school it will be removed and placed in the school office for collection at home time.

### **Staff Use of Personal Devices**

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- Mobile Phones and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

## 1.5 Communication Policy

### 1.5.1 How will the policy be introduced to pupils?

- This e-safety policy has been discussed with the school council and the children's acceptable use policy has been agreed.
- All users will be informed that network and Internet use will be monitored.
- An e-Safety training programme has been established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- An e-Safety module is included in computing lesson and assemblies half termly covering both safe school and home use.
- e-Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
- e-Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

Useful e–Safety programmes include:

- Think U Know: [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)
- Childnet: [www.childnet.com](http://www.childnet.com)
- Kidsmart: [www.kidsmart.org.uk](http://www.kidsmart.org.uk)
- Orange Education: [www.orange.co.uk/education](http://www.orange.co.uk/education)
- Safe: [www.safesocialnetworking.org](http://www.safesocialnetworking.org)

### 1.5.2 How will the policy be discussed with staff?

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

### 1.5.3 How will parents' support be enlisted?

- Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days.
- Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss it's implications with their children.
- Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations listed in the “e–Safety Contacts and References section”.

## **e-Safety Contacts and References**

**CEOP** (Child Exploitation and Online Protection Centre): [www.ceop.police.uk](http://www.ceop.police.uk)

**Childline:** [www.childline.org.uk](http://www.childline.org.uk)

**Childnet:** [www.childnet.com](http://www.childnet.com)

**Click Clever Click Safe Campaign:** <http://clickcleverclicksafe.direct.gov.uk>

**Cybermentors:** [www.cybermentors.org.uk](http://www.cybermentors.org.uk)

**Digizen:** [www.digizen.org.uk](http://www.digizen.org.uk)

**Durham EDS** – E-safety, Teaching and learning advice Tel: 0191 3834370

**Durham Safeguarding Children Board** (DLSCB): [www.durham-lscb.gov.uk](http://www.durham-lscb.gov.uk)

**ICT Service Desk** – Changes to filtering Tel: 03000 261100

**ICTSS Service Desk** – All other ICT issues Tel: 01388 424999

**Internet Watch Foundation** (IWF): [www.iwf.org.uk](http://www.iwf.org.uk)

**Kent e–Safety in Schools Guidance:** [www.kenttrustweb.org.uk?esafety](http://www.kenttrustweb.org.uk?esafety)

**Kidsmart:** [www.kidsmart.org.uk](http://www.kidsmart.org.uk)

**Schools e–Safety Blog:** [www.kenttrustweb.org.uk?esafetyblog](http://www.kenttrustweb.org.uk?esafetyblog)

**Teach Today:** <http://en.teachtoday.eu>

**Think U Know website:** [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

**Virtual Global Taskforce** — Report Abuse: [www.virtualglobaltaskforce.com](http://www.virtualglobaltaskforce.com)