Ellington Primary School

E-Safety Policy

What is e-safety?

E-safety encompasses the use of new technologies, internet and electronic communications such as mobile devices, digital cameras, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The School's e-safety policy reflects the need to raise awareness of the safety issues associated with electronic communications as a whole.

The school's e-safety policy will operate in conjunction with Northumberland County Council's guidance in 'On-line Safety and Security in Schools' and other policies including Computing, Behaviour, Anti-bullying, Curriculum, Data Protection and Security and PREVENT.

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

- Responsible computing use by all staff and pupils; encouraged by education and made explicit through published policies that include the Staff Acceptable Computing Use Agreement (staff) and Rules for Responsible Internet Use (pupils).
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Northumberland County Council including the effective management of filtering.
- National Education Network standards and specifications.

Ellington Primary School E-Safety Policy

Ellington Primary School's e-safety policy is part of the School Development Plan and relates to other policies including those for computing, bullying and for child protection.

- The school's e-safety co-ordinators are Mr K Hodgson (Headteacher) and Mrs R Richardson. (Computing co-ordinator)
- Mrs D Towers is the named governor for e-safety.
- The school's designated safeguarding lead is Mr Hodgson. (Headteacher)
- Mrs Pirie (Deputy Headteacher) is also a designated safeguarding lead.
- Mrs D Towers is the named governor for child protection.

Our E-Safety Policy has been written by the school, built on information from e-safety training provided by Northumberland County Council and government guidance.

- The policy has been agreed by senior management and approved by governors.
- The policy and its implementation will be reviewed annually.
- The e-safety Co-odinator liaises with the computing team and technical Support person to provide day to day support for staff
- Mr K Hodgson, Mrs R. Richardson and Mr D. Mathewson make up the e-safety team.

Teaching and learning

Why Internet use is important

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school's internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils (provided by Northumberland County Council).
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for e-safety and take part in national e-safety weeks.
- 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 how to evaluate Internet content

- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly in conjunction with Northumberland County Council.
- Virus protection will be updated regularly in conjunction with Northumberland County Council.
- Security strategies will be discussed with Northumberland County Council.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mails.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school website

- The contact details on the Website are the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully.
- Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.
- Parents or carers will have the opportunity to request that photographs of their children are not published on the school Website.
- Photographs of children are held securely until the child has left school, when they are deleted, unless they are of interest to the school archives.
- Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- The school will block access to social networking sites except for Twitter, for staff use only.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network, cyberbullying and posted digital images (that stay on the internet) outside school is inappropriate for primary aged pupils.

Managing filtering

- The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-safety coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

School will use Google Meet to conduct any video conferencing. No links to any meetings will be shared publicly.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Children from Nursery to Year 4 are not permitted to bring mobile phones into school.
- Children in Years 5 and 6 can bring a mobile phone into school but these must be handed in to their class teacher and securely stored until home time, before being handed back out.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (May 2018).
- Data must be encrypted and password protected.

Policy

Authorising Internet access

- All staff must read and sign the 'Acceptable Computing Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At EYFS, Key Stage 1 and 2, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.
- Inappropriate use of the internet will be dealt with in line with the school's behaviour and anti-bullying policies.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Northumberland County Council can accept liability for the material accessed, or any consequences of internet access.
- The school will audit Computing provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff (e-safety officer).
- Any complaint about staff misuse must be referred to the headteacher.
- 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.

Community use of the Internet

- Any adults using school internet facilities will be required to sign the 'Staff Acceptable Computing Use Agreement' and will have access to this e-safety policy.

Communications Policy

Introducing the E-Safety policy to pupils

- E-safety rules will be posted beside all computer areas in school and they will be discussed with the pupils at the start of each year.
- Pupils will be informed that Network, Learning Platforms and Internet use will be monitored.
- Pupils will be taught about the dangers of using the Internet at an age appropriate level.

Staff and the e-safety policy

- All staff will be trained and have access to the school e-safety policy and have its importance explained.
- Staff should be aware that internet traffic is monitored by SENSO. Discretion and professional conduct is essential.
- Staff should be good role models in the use of technology including the internet and social media.
- Staff should not have access to the school's internet on personal devices.

Enlisting parents' support

- Parents'/Carers', grandparents and childminders' attention will be drawn to the School e-Safety Policy in newsletters, on the school Website, Curriculum Evenings and high profile events e.g. Internet Safety Day.

E-Safety Audit

This quick audit will help the senior management team (SMT) assess whether the basics of e-safety are in place. Schools will also design learning activities that are inherently safe and might include those detailed within Appendix 1.

The school has an e-Safety Policy that complies with CFE guidance.	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at	
And for parents at	
The Designated Child Protection Coordinator is	
The e-Safety Coordinator is	
How is e-Safety training provided?	
Is the Think U Know training being considered?	Y/N
All staff sign an Acceptable Computing Use Agreement on appointment.	Y/N
Parents sign and return an agreement that their child will comply with the school Acceptable Computing Use statement.	Y/N
Rules for Responsible Use have been set for students:	Y/N
These Rules are displayed in all rooms with computers.	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access.	Y/N
The school filtering policy has been approved by SMT.	Y/N
A computing security audit has been initiated by SMT, possibly using external expertise.	Y/N
School personal data is collected, stored and used according to the principles of the Data Protection Act.	Y/N
Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by a member of SMT.	Y/N

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks Webquest UK Kent Grid for Learning (Tunbridge Wells Network)
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. - Ask Jeeves for kids - Yahooligans - CBBC Search - Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	RM EasyMail SuperClubs PLUS Gold Star Café School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	Making the News SuperClubs Infomapper Headline History Kent Grid for Learning Focus on Film
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Making the News SuperClubs Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Skype FlashMeeting
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail	Skype FlashMeeting National Archives "On-Line" Global Leap

	address or protected password should be used.	National History Museum Imperial War Museum