Ref/CS/MS

Prudhoe West First School

E-Safety Policy 2014/15

September 2014

Prudhoe West First School

E-Safety Policy 2014

Why does a School need an e-Safety Policy?

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

E-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

The balance between controlling access to the Internet and technology, setting rules and boundaries and educating students and staff about responsible use is an important consideration. Our pupils are empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff are aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff are informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

The e-Safety policy is essential in setting out how the school plans to develop and establish its e-Safety approach and to identify core principles which all members of the school community need to be aware of and understand.

The Headteacher and Governing body have a legal responsibility to safeguard children and staff and this includes online activity.

- The e–Safety Policy and its implementation will be reviewed annually.
- Our e–Safety Policy has been written by the school, building on the Kent County Council e–Safety Policy and government guidance.
- Our School Policy has been agreed by the Senior Leadership Team and approved by governors.

The School e-Safety Coordinator is Mrs M Smith
Policy approved by Head Teacher Date: 025/09/14

Policy approved by Governing Body: (Chair of Governors)
Date: 07/07/14

The date for the next policy review is September 2015

Teaching and learning

Why is Internet use important?

The rapid developments in electronic communications are having many effects on society. It is important to state what we are trying to achieve in education through ICT and Internet use.

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday 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.
- 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.

Using the Internet to 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;
- inclusion in the National Education Network which connects all UK schools;
- 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 Northumberland County Council and DfE;
- access to learning wherever and whenever convenient.

Enhancing learning with the use of the Internet

Developing effective practice in using the Internet for teaching and learning is essential. Digital Literacy is an integral part of the new Computing curriculum. Pupils need to learn Digital Literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught.

- The school's Internet access will be designed to enhance and extend education.
- Maths and spelling homework will be set using the Mathletics and Spellodrome programs, both of which can be accessed at home via the Internet. Each pupil will receive their own personal log in, to access homework set specifically for themselves by their own class teacher.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils must accept the school's Acceptable Use Policy at log on to the network. For reasons of online safety, all users should understand that network activity and online communications are monitored using Policy Central Enterprise.

- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Access levels to the Internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- 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.

Teaching pupils to learn how to evaluate Internet content

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read.

- 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 use age-appropriate tools to research Internet content.

Managing Information Systems

How will information systems security be maintained?

Local Area Network (LAN) security issues include:

  - Users must take responsibility for their network use.
  - Server access is restricted to authorised users.
  - The server operating system is secured, backed up and kept up to date.
  - Virus protection for the whole network is installed and current.
  - Access by wireless devices is proactively managed and secured with a WPA2 encryption.

- The security of the school information systems and users will be reviewed regularly.
- Virus protection is automatically updated.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not used without specific permission followed by an anti-virus / malware scan.
- Unapproved software is not allowed in work areas or attached to emails.
- Files held on the school's network will be regularly checked.
- The use of user logins and passwords to access the school network is enforced.

Managing e-mail

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits; interesting projects between schools in neighbouring villages and in different continents can be created.

The implications of email use for the school and pupils need to be thought through and appropriate safety measures put in place.

It is important that staff understand they should be using a work provided email account to communicate with parents/carers, pupils and other professionals for any official school business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a 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.

Managing published content

- The contact details on the website are the school address, email and telephone number.
- 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 privacy policies, Data Protection Act 1998 and copyright.

Publishing pupil's images and work

At Prudhoe West First School we sometimes take photographs of pupils either at school or when they are involved in organised activities away from the school site. We use these photographs of pupils to record their learning and track their progress. From time to time we also use photographs in our prospectus or in other printed publications we produce as well as our website or on school displays.

For key events in the life of the school, the media may visit and may take photographs, film footage or carry out radio interviews. Pupils will often appear in these photographs or films, which may appear in local or national newspapers, or on televised news programmes.

We are of course; committed to safeguarding and promoting the welfare of our pupils in all aspects of school life and therefore we need to comply with the Data Protection Act 1998. To do this we need written permission to photograph or make any recordings of our pupils.

Furthermore, we are required by law to bring to our parents/carers attention that they are not permitted to take photographs or make recordings featuring anyone but their own children for anything other than their own personal use. To do so, such as posting photographs featuring other people's children on Facebook, Twitter or similar, would require consent of the other children's parents/carers, and if this was not given would mean parents/carers concerned would be in breach of the Data Protection Act 1998.

- 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 the 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.

Managing social networking, social media and personal publishing

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples of social media and personal publishing tools include: blogs, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

- There is no access to social media and social networking sites in school.
- 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, instant messaging and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff official blogs must be password protected and run from the school website with approval from the Senior Leadership Team.
- 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.
- Staff personal use of social networking, social media and personal publishing sites is discussed as part of staff induction and safe and professional behaviour is outlined in the school Acceptable Use Policy.

Managing Filtering

Levels of Internet access and supervision will vary according to the pupil's age and experience.

- The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- In the event of an e-safety incident, the procedures outlined in the Northumberland Safeguarding Children's Board flowchart must be followed.
- The school's SLT will ensure that regular checks on network monitoring are made using Policy Central Enterprise to ensure that the filtering methods selected are appropriate, effective and reasonable.

Occasionally mistakes may happen and inappropriate content may be accessed. It is therefore important that children should always be supervised when using internet access and that Acceptable Use Policies are in place. In addition, Internet Safety Rules should be displayed, and both children and adults should be educated about the risks online.

Teachers should always evaluate any websites/search engines before using them with their pupils; this includes websites shown in class as well as websites accessed directly by the pupils

- The school's broadband access includes filtering appropriate to the age and maturity of pupils.
- The school will work with Northumberland LA and the Schools Broadband team to ensure that the filtering policy is continually reviewed.

- 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. (See attached Northumberland Safeguarding Children's Board flowchart)
- 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.
- Any material that the school believes is illegal will be reported to appropriate agencies such as Northumbria Police or CEOP.

Managing videoconferencing

Videoconferencing enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in education.
Equipment ranges from small PC systems (web cameras) to large room-based systems that can be used for whole classes or lectures.

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

Users

- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- 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.
- 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.

Managing emerging technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken by the Computing Co-ordinator when new technology is purchased, to ensure effective and safe practice in classroom use to be developed.

New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access.

Schools should keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies. Staff should never use personal phones to contact pupils or parents/carers.

Pupils are not allowed mobile phones in school. (See mobile phone policy).

- 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 Policy.

Protecting personal data

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

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.

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. Staff filling in Reception profiles which contain personal data and are shared with parents via the Internet must follow its guidelines.

Policy Decisions

Authorising Internet access

The school allocates Internet access to staff and pupils on the basis of educational need.

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff will read and sign the 'Staff Information Systems Code of Conduct' or 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 children with special education needs) the school will make decisions based on the specific needs and understanding of the pupils.
- Foundation Stage pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- At Key Stage 1 & 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

Assessing risks

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation.

- 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 Northumberland LA 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 Northumbria Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Responding to any incidents of concern

Internet technologies and electronic communications provide children and young people with exciting opportunities to broaden their learning experiences and develop creativity in and out of school. However it is also important to consider the risks associated with the way these technologies can be used.

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, school should refer to the procedures outlined in the Northumberland Safeguarding Children's Board flowchart to determine the level of response necessary for the offence disclosed. The decision to involve Police should be made as soon as possible, after contacting the Children Safeguard Team or e-Safety officer, if the offence is deemed to be out of the remit of the school to deal with.

- 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 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 of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

Handling e–Safety complaints

The facts of the incident or concern will need to be established and evidence should be gathered where possible and appropriate. E-Safety incidents may have an impact on pupils; staff and the wider school community both on and off site and can have civil, legal and disciplinary consequences.

- 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.
- 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.

Managing Cyber Bullying

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

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyber bullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

- Cyber bullying (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.
- All incidents of cyber bullying reported to the school will be recorded.
- 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.

Managing Learning Platforms

An effective learning platform or learning environment can offer schools a wide range of benefits to teachers, pupils and parents, as well as support for management and administration. It can enable pupils and teachers to collaborate in and across schools, sharing resources and tools for a range of topics. It also enables the creation and management of digital content and pupils can develop online and secure e-portfolios to showcase examples of work.

The Learning Platform/Environment (Nortle) must be used subject to careful monitoring by the Senior Leadership Team (SLT).

SLT and staff will regularly monitor the usage of the Nortle 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 Nortle.
- Only members of the current pupil and staff community will have access to Nortle.
- 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 Nortle 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 Nortle for the user may be suspended.
d) A pupil's parent/carer may be informed.

Managing mobile phones and personal devices

Mobile phones and other personal devices such as Games Consoles, Tablets, PDAs and MP3 Players etc. are considered to be an everyday item in today's society. Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet access all common features.

Due to the widespread use of personal devices it is essential that schools take steps to ensure mobile phones and devices are used responsibly at school and it is essential that pupil use of mobile phones does not impede teaching, learning and good order in classrooms. Staff should be given clear boundaries on professional use.

- The use of mobile phones in school by pupils is prohibited. 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.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools.

Communication Policy

Introducing the policy to pupils

Many pupils are very familiar with culture of mobile and Internet use. The e–Safety rules will be explained and discussed.
The teaching of e–Safety is incorporated into the Computing Scheme Of Work across all key stages.

- All users will be informed that network and Internet use will be monitored.
- An e–Safety training programme will be 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.
- 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.

Discussing the e-Safety Policy with staff

It is important that all staff feel confident to use new technologies in teaching and the
School E–Safety Policy will only be effective if all staff subscribe to its values and methods.

Computing use is widespread and all staff including administration, midday supervisors, caretakers, governors and volunteers should be included in awareness raising and training. Induction of new staff includes a discussion about the school E–Safety Policy.

- The E–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school has implemented an Acceptable Use Policy.

- 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 Computing use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.

Enlisting parents' support

Internet use in pupils' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home.

- Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.
- 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.

M. Smith/C Speed

Established	September 2011
Reviewed	September 2014
Review	September 2015

Prudhoe West First School

Staff ICT Acceptable Use Policy 2013

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …… Print Name: ……..

Date: ……