## 1.RATIONALE

- At Acomb First School we believe that the use of ICT and the Internet are valuable resources to both teachers and pupils and can help raise standards. Recognising the dangers and planning the use of suitable resources is vital to safe guarding children in our school. Our aim is to promote safe use of ICT and Internet resources, through developing pupil, parent and teacher awareness. We have established clear mechanisms to identify, intervene and respond appropriately and quickly to an incident, where appropriate.

## 2.WHY IS E-SAFETY IMPORTANT?

Accessing the Internet in schools has gone beyond just the use of desktop computers. To protect young children effectively we aim to identify the numerous ways in which children access the internet, both at school and at home. Informing both children and their parents will be key to tackling E-safety through identifying ways in which children access the Internet and ways of protecting the children from potential risks whilst online. This policy document aims to educate children and parents of ways the Internet can be used safely. Children working online in school or at home should understand the risks they face and should be equipped with strategies to deal with issues.

This policy document aims to educate children and parents of ways the Internet can be used safely. Children working online in school or at home should understand the risks they face and should be equipped with strategies to deal with issues. At Acomb First School we aim to develop an awareness through the use of our Acceptable Use Policy (AUP) and pupil/parent agreement. Teachers, children and parents will receive information to highlight factors they should consider when using ICT equipment and the Internet. Posters highlighting key E-Safety responsibilities for children/adults will be displayed throughout the school to remind the importance of safety first.

## 3. ROLES AND RESPONSIBILITIES

### The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

All governors will: ensure that they have read and understand this policy, agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.

### The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

### The E safety lead

In cooperation with the head teacher takes lead responsibility for online safety in school, in particular:

•ensuring that staff understand this policy and that it is being implemented consistently throughout the school

•Working with the headteacher, and other staff, as necessary, to address any online safety issues or incidents

•Ensuring that any online safety incidents are logged in the child protection log and dealt with appropriately in line with this policy

•Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

•Updating and delivering staff training on online Safety

•Liaising with other agencies and/or external services if necessary

**School Staff**

Due to continual developments in computing and E-Safety, planning and practice need to be assessed and changed to suit the needs of the children in our school. At Acomb First School it is essential that the staff are briefed on procedures that will allow them to deal with discussions about children's Internet use. Through the use of INSET staff will receive the necessary training and advice in order to combat problems children in their class may face. Advice and training may be obtained from outside agencies/advisors such CEOP. Courses that promote E-Safety will be attended by the E Learning subject leader in order to continue to develop strategies to enhance E-safety in our school. Key information will be fed back to the staff. The school ethos encourages trust between staff, pupils and parents/guardians.

As child educators it is part of our role that we safeguard children in our care and educate them about how to safely use IT both in and out of school.

The Child Exploitation and Online Protection centre (CEOP) has been set up by the Home Office to "safeguard children's online experiences and relentlessly track down and prosecute offenders". All staff members are required to sign an Acceptable ICT Use Agreement on appointment and thereafter on an annual basis. In signing, staff members accept that the school can monitor network and Internet use to help ensure staff and pupil safety.

Staff will report inappropriate use of technology that they are made aware of to Angela Speed (Head teacher/ designated Safeguarding Lead) or Fiona Hinchcliffe E-Safety Lead/ Deputy Safeguarding Person. Senior management will follow set procedures and investigate incidents with care and attention, with an understanding that there may be an innocent explanation. Staff will be briefed on the dangers of mis-management of ICT, for example, the potential for children to view inappropriate images if a search engine is used during a lesson without prior planning.

A Northumberland email accounts will be issued to new members of staff or current members of staff that do not currently possess an account for sharing of information. The E-Mail accounts are password protected. The use of personal mobile phones is prohibited during teaching time when phones should be switched off, unless on educational visits. Personal mobiles must not be used to store images of children.

Staff will be mindful of where they store personal data. All documents containing personal data should be stored on the school team drive. It should never be stored on portable devises such as laptops, USB drives, IPads, hard-drives or on staff computers. When data is being accessed staff should ensure that linked smart-boards are switched off. Data should never be left on computer screens when not in use. Photographs should be stored on the team drive and then immediately wiped from Ipads.

## 4. ROUTES TO E-SAFETY

Despite precautions at school, open access to the Internet has become an integral part of children's lives. A growing danger is presented by the ease of uploading material to the Web. We are aware of primary pupils' use at home of social networking sites which allow children to set up an account and create a web page in minutes. Information given by users is not checked and there appears to be a total lack of safeguards. Through planned lessons, children will develop a better insight into the meaning of 'e-Safety.

### What Does Electronic Communication Include?

- **Internet collaboration tools:** social networking sites and blogs
- **Internet Research**: web sites, search engines and Web browsers
- **Mobile Phones and personal digital assistants** (PDAs)
- **Internet communications:** e-Mail and instant messaging (IM)
- **Webcams and videoconferencing**

### What Are The Risks?

- Receiving inappropriate content
- Predation and grooming
- Requests for personal information
- Viewing 'incitement' sites
- Bullying and threats
- Identity theft
- Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information / images
- Hacking and security breaches
- Radicalisation

## 5. **PARENTAL INVOLVEMENT**

Working alongside parents/guardians is vital when promoting e-safety, as children can spend a lot of time using ICT in their homes, such as Internet browsing, chat rooms, messenger facilities, games consoles, etc. Providing parents with the appropriate information regarding safeguarding their children is essential. Key areas to be focused on will be:

- Mobile phone

- Internet grooming

- Gaming websites or consoles that can be attached the Internet.

- Social networking sites

- Chat forums or blogs

Through assemblies, parents meetings and the school website parents will be provided with information on how to keep their children safe online. The school website provides a link to the 'Report Abuse' facility on 'Think You Know' homepage and other safety information. Parents are provided with information about how we intend to promote e-safety in school and the rules/contract we will implement. Resources, information and advice will be made available to parents regarding how to promote safe-use in their homes. As part of our home school agreement will ensure that a copy of the School's e-Safety Policy is sent to parents and governors

## 6. IDENTIFYING VULNERABLE GROUPS

Many primary pupils have access to mobile devices. The use of internet-enabled mobile phones, tablets and games consoles outside school is increasing rapidly. The most ICT capable may be the most vulnerable. Children who interact poorly socially may be more at risk from inappropriate online contact. Staff will log any concerns the might have regarding inappropriate use of ICT using safeguarding incident forms and inform Safeguarding Lead.

## 7. USING THE INTERNET TO SUPPORT LEARNING

The use of Internet sites is essential to teaching and staff members are encouraged to use safe, purposeful sites that are beneficial to learners. Through the use of the School 360 **Homepage'**, websites are recommended that contain suitable content to assist teaching and learning. We recognise that there is always an element of risk: even an innocent search can occasionally turn up links to adult content or violent imagery. For the youngest pupils, the greatest risk is through inadvertent access. Fast broadband means that inappropriate images can appear almost instantaneously. Children can innocently follow a series of links to undesirable content. In order to combat this issue a procedure has been agreed by staff of how to handle the situation with pupils. Teachers will be advised to:

- **Tell children to minimize the screen immediately.**
- **Do not navigate away from the screen.**
- **Talk to children about what has happened and reassure them they are not in trouble.**
- **Later investigate the history of the sites visited to get details of the inappropriate site and how the child got there.**
- **Report the incident using the appropriate form.**

In light of potential problems when accessing Internet sites or search engines, primary pupils are not permitted to use the Internet in school unless they are supervised by an adult at all times. Children will log on using either their own log in. The requirement to log in allows Northumberland monitoring software to track the websites visited and a report is sent to senior management recording any inappropriate searches. Acomb First School has up to date filters and security programs installed as part of their ICT provision from Northumberland in an aim to reduce the chance of children accessing websites with inappropriate content.

## INFORMATION SYSTEMS INTEGRITY AND SECURITY

At Acomb First School the administration network has access to the Northumberland County Council Intranet, this is not accessible externally. A firewall is in place and prevents access from external sites to the curriculum network. Administration computers are protected via an Internet Service Provider (ISA) Server at our school and other ISA servers at County Hall.

The broadband link is provided by the Northumberland County Council via the Internet Service Providers (ISP) to our schools administration network.

Antivirus software is installed throughout our school and is regularly updated. Staff desktops, staff laptops and children's desktops are protected by E-Safety antivirus software provided by the NCC.

**15. MAINTENANCE**

Part of our investment into ICT has been to employ a technician from NCC.  A technician visits the site for half a day monthly. The technician completes numerous jobs including anti-virus checks, installing software and generally making systems more user friendly and efficient.