Ashleigh Primary School and Nursery, Wymondham

"We are all stars, Ashleigh makes us shine"

E-SAFETY POLICY

Persons Responsible – Senior Leadership Team, Governors

Date of Policy: May 2015 **Next Review Due: May 2018**

Adopted by Full Governing Body

Signed ..... **Date** .....

Chair of Governors

Review completed .....

Review completed .....

Review completed .....

What is E-safety?

Pupils interact with the internet and other communications technologies such as mobile phones on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas and social interaction are both greatly beneficial but can occasionally place young people in danger.

E-safety comprises all aspects relating to children and young people and their safe use of the Internet, mobile phones and other technologies, both in and out of school. It includes education on risks and responsibilities and is part of the 'Duty of Care' which applies to everyone working with children. A new national e-Safety drive is being led by the Child Exploitation and Online Protection Centre (CEOP).

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology and provides safeguards and awareness for users to enable them to control their online experiences.

The internet is an open communications channel, available to all. Applications such as the web, e-mail, blogs and social networking all transmit information over the fibres of the Internet to many locations in the world at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the internet make it an invaluable resource used by millions of people every day.

Some of the material on the internet is published for an adult audience and is unsuitable for pupils. For instance, there is information on weapons, crime and racism that would be more restricted elsewhere. It is important that pupils are made aware of appropriate behaviour in relation to contacting others and they must also understand that publishing personal information could compromise their security.

Responsibility, regulation and compliance
Our e-safety policy has been agreed by the senior management and approved by governors and the PTA. The e-Safety Policy will be reviewed annually.

All staff at Ashleigh Infant School are required to sign an Acceptable ICT User Agreement on appointment. This includes trainee teachers and NVQ students who have access to the systems in school. In signing this agreement, staff accept that the school can monitor network and internet use to help ensure staff and pupil safety.

The school keeps an up-to-date record of access levels granted to all network users. Parents are informed that students are provided with supervised internet access and parents and pupils are required to sign an acceptable use agreement upon entering the school. Senior staff take responsibility for regularly checking that filtering and monitoring is appropriate, effective and reasonable.

Both staff and students understand that the use of the school's network is a privilege which can be removed should reason arise. The school monitors all network and internet use in order to ensure student safety.

There is an underlying assumption that children have both understanding and application of "safety". Pupils need to understand that rules given to them must be followed. Pupils need to learn safety rules in a way that does not frighten them and which gives them confidence to know what to do in certain situations. Pupils need to understand that certain rules will change and develop as they get older.

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 business administration systems. Internet access is an entitlement for pupils who show a responsible and mature approach to its use. The school has a duty to provide pupils with safe and secure internet access as part of their learning experience. The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.

E-Safety depends on staff, schools, governors, advisers and, in particular, parents and the pupils themselves taking responsibility. Staff have a particular responsibility to supervise use, plan access and set good examples. The balance between educating pupils to take a responsible approach and the use of regulation must be judged carefully.

All users are expected to adhere to the generally accepted rules of network etiquette (netiquette). These include, but are not limited to, the following:

- Be polite.
- Use appropriate language.
- Do not reveal the personal address, phone number or other personal details of yourself or other users.
- System administrators have access to all mail.

- Messages relating to or in support of illegal activities may be reported to the authorities.

No policy can protect pupils by itself. Staff vigilance in planning and supervising appropriate and educational ICT experiences remains essential. The security of the school information systems will be reviewed regularly. These include:

- Anti-virus protection is installed on all computers and updated regularly.
- The school uses the Norfolk broadband with its firewall and filters.
- The school provides an additional level of protection through its deployment of Policy Central in partnership with Norfolk County Council ICT Shared Services.
- Portable media is only used with specific permission, password protection and a virus check.
- Unapproved system utilities and executable files are not allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network are regularly checked.
- The IT co-ordinator reviews the system capacity on a regular basis.
- The school maintains a current record of all staff and pupils who are granted Internet access.
- All staff must read and abide by the 'Acceptable ICT Use Policy' before using any school ICT resource.
- At Key Stage 1, access to the Internet is by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents are informed that pupils will be provided with supervised Internet access
- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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 NCC can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The head teacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.
- Rules for Internet access is posted in all networked rooms.
- Staff and pupils are informed that Internet use will be monitored.
- An e-Safety training programme aimed at pupils is in place in all year groups to raise the awareness and importance of safe and responsible Internet use.
- A module on responsible Internet is also included in the PSHE and ICT programmes covering both school and home use.

Managing teaching and learning

- 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 business administration systems.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- 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.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;
- Educational and cultural exchanges between pupils world-wide;
- 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 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 the LA and DfE;
- Access to learning wherever and whenever convenient.

Good planning and preparation is critical in ensuring a safe starting point for the development of Web search skills and strategies. Tasks can be planned that do not require an Internet-wide search engine.

If the aim is to teach search skills, BBC Schools offers a safe environment. The search box automatically restricts the search to the BBC Schools site. There is no indication of age range, but pupils can judge readability from the example retrieved by the search www.bbc.co.uk/schools. Importantly, primary pupils can learn skills such as keyword selection to narrow down searches, and evaluating quality and relevance. This will prepare them for efficient, productive Internet research in the secondary phase. It is also possible for staff to create links to websites by dragging the icon from the address bar in Internet Explorer into the web-links folder in the shared area. Pupils would then be able to access the site by clicking the link.

Most internet use in primary schools is safe, purposeful and beneficial to learners. However, there is always an element of risk: even an innocent search can occasionally

turn up links to adult content or violent imagery, that are not filtered out by the security systems in place.

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. **If this happens, a responsible adult should close or minimise the window immediately and not try to navigate away. If the image has been view on an iPad the device should be taken from the pupil. The home and lock key should then be used to take a photograph of the page for recording and logging use by the e-safety co-ordinator. If the pupil saw the page, the adult should talk to them about what has happened and reassure them. Later, the adult should investigate the history of visited sites to get details to report, and to find out how the pupil got there. If possible a screen shot should be taken. The matter should also be reported to the ICT co-ordinator so that the web site can be added to the centrally controlled filtered list.**

In view of these risks, Ashleigh pupils are supervised at all times when using the internet. Staff are aware that networked computers are online at all times when a user is logged on and are trained to research search results that pupils may encounter prior to lessons.

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to ICT shared services.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

Managing electronic communication

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
- Wireless games consoles
- IPads

What are the risks?

- Receiving inappropriate content
- Predation and grooming
- Requests for personal information
- Bullying and threats
- Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information
- Identity theft
- Hacking and security breaches
- Corruption or misuse of data
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Use of words included in the Policy Central 'banned' list will be detected and logged.
- Whole-class or group e-mail addresses are available for use with younger children.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and may be restricted.
- E-mail sent to external organisations should be written carefully and authorisation may be required before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters, by staff or pupils is not permitted.
- Staff are advised not to provide their personal email address to children or parents of children, currently at the school.
- Staff are advised to only use their school email address accessed via the learning platform for work related use.
- Staff are not permitted to use their school email address for personal use and emails are monitored centrally.
- Staff are advised that personal emails cannot be accessed on school's devices
- Photographs that include pupils will be selected carefully and only used with express written permission from parents (a parent consent form is provided upon school entry).
- Staff are not permitted to take photographs of children on their personal mobile phones or cameras.
- All staff are provided with a school camera which remains on site
- Photographs taken using the iPads must be cleared off the memory within 24 hours of being taken

Social networking

- Social networking sites and newsgroups will be blocked unless a specific use is approved
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, school or shopping centre.
- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers are advised not to run social network spaces for students on a personal basis.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others.
- Pupils should be advised not to publish specific and detailed private thoughts.
- Staff are made aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.
- Staff are advised not to make links with children or parents of children currently at the school, on social networking sites.
- Staff are advised that posting inappropriate information on social networking sites may be detrimental to their position of employment and should take precaution when using such sites.

Mobile phones

- Staff are able to use a school phone when on site where contact with parents is required.

Managing personal data

The Data Protection Act gives individuals the right to know what information is held about them and it 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 an individual). The act also gives rights to the people the

information is about i.e. the right of subject access, lets individuals find out what information is held about them.

The eight principles are that personal data must be:
1. Processed fairly and lawfully
2. Processed for specified purposes
3. Adequate, relevant and not excessive
4. Accurate and up-to-date
5. Held no longer than is necessary
6. Processed in line with individuals rights
7. Kept secure
8. Transferred only to other countries with suitable security measures.

In compliance with the Data Protection Act, teachers are required to sign a Data Security Agreement, concerning the transfer of information about pupils. This agreement states that:
Sensitive information contain personal details must be encrypted with a password before being transferred using a USB memory stick. Staff home/personal computers must be password protected if such details are stored on the hard drive.

Sensitive information includes:
- SEN information (IEPs, minutes of meetings, notes from support agencies)
- Reports on pupils
- Class lists which have surnames and/or dates of birth on them
- Assessment information which holds a child's full name

Response to concerns/complaints
Any concerns or complaints relating to E-safety should be reported to the ICT Coordinator or the Designated Child Protection Coordinator. Any complaint about staff misuse must be referred to the head teacher who will follow agreed NCC procedures. Pupils and parents are informed of the complaints procedure and pupils will need to work in partnership with designated staff to resolve issues.

The school will review this policy regularly and revise it annually to ensure that it is current and includes any emerging technologies used in school. The school will audit their filtering systems regularly to ensure that inappropriate websites are blocked and that pupils and staff are adhering to the policy, by investigating any incidents of misuse.

The school includes e-Safety in the curriculum and ensures that every pupil has been educated about safe and responsible use. Every pupil knows how to control and minimise online risks and how to report a problem. The school has an Acceptable Use Policy and encourages its adoption by all staff and students. Parents are required to sign and return the consent form for Responsible Internet Use. All staff, governors, parents and visitors have access to a copy of this policy to read and review.

Relevant Government legislation

- The Computer Misuse Act 1990 - makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.
- Public Order Act 1986 – offence to possess, publish, disseminate material intended to/likely to incite racial hatred.
- Communications Act 2003 - There are 2 separate offences under this act:

a) sending by means of a public electronic communications network, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character.
b) sending of a false message or persistently making use of a public electronic communications network for the purpose of causing annoyance, inconvenience or needless anxiety.

- This wording is important because the offence under **a)** is complete when the message has been sent - no need to prove any intent or purpose. It is an offence under **b**) to keep using the network for sending any kind of message irrespective of content if for the purpose of causing annoyance etc.
- Malicious Communications Act 1988 – offence to send a letter, electronic communication or article which is indecent or grossly offensive, threatening or false information with intent to cause distress or anxiety to the recipient.
- Copyright, Design and Patents Act 1988 - it is an offence to use unlicensed software
- Protection of Children Act 1978 - The law on images of child abuse is clear. It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom.
- Obscene Publications Act 1959 and 1964 - defines "obscene" and related offences.
- Protection from Harassment Act 1997
- Section 2 - A person must not pursue a course of conduct, which amounts to harassment of another.
- Section 4 - A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Monitoring School ICT Use

Monitoring network activity could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998.

The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic

monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day to day activities.

Ashleigh Infant School may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others. Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.

The Rules for Responsible Internet Use, with which every user agrees to comply, contains a paragraph that should ensure users are aware that the school is monitoring Internet use.
In order to defend claims that it has breached either the 2000 Regulations or the Human Rights Act 1998, a school should devise procedures for monitoring, ensure monitoring is supervised by a senior manager and maintain a log of that monitoring.

Sex Offences Act 2003 Memorandum of Understanding
Memorandum of Understanding Between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) concerning Section 46 Sexual Offences Act 2003.

The aim of this memorandum is to help clarify the position of those professionally involved in the management, operation or use of electronic communications networks and services which may face jeopardy for criminal offences so that they will be re-assured of protection where they are acting to combat the creation and distribution of images of child abuse. This memorandum has been created within the context of child protection, which will always take primacy.