E-Safety Policy

Who will write and review this policy?
• The school has an appointed e-safety governors, who together with the ICT coordinator will ensure that the policy is reviewed, along with reviewing current practice, policy implementation and dealing with any e-safety issues that may arise.
• This e-safety policy and its implementation will be reviewed by the governors in line with their policy review timetable.

Teaching and Learning

Why is Internet use important?
• 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 use is part of the statutory curriculum and a necessary tool for learning.
• The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
• We recognise that many 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.

How does Internet use benefit education?
Benefits of using the Internet in education include:
• Access to world-wide educational resources including museums and art galleries
• 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 online 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.

How will pupils learn how to evaluate Internet content?
• Key Stage 1 pupils will be supervised when using the Internet and taught what to do if they get lost on the Internet and if they come across anything that they don't like.
• Key Stage 2 pupils will be taught to search for and discriminate between valid and inappropriate material e.g. being aware of key information such as author's name, date of revision and links to other sites as well as comparing the material with that of other sites.
• Pupils will be taught to copy, save and use material found on the Internet without infringing copyright.

Managing Information Systems

How will information systems security be maintained?
• The security of the school information systems will be reviewed regularly.
• Virus protection will be updated regularly.
• Personal data sent over the internet will be encrypted or otherwise secured
• Portable media may not be used without specific permission followed by a virus check.
• Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
• Files held on the school's network can be easily accessed and will be regularly checked.
• The ICT co-ordinator will review system capacity regularly.
• Access codes and passwords for school network will not be given to anyone who is not authorised to use the school system and these will not be passed on to anyone else by members of staff.

How will e-mail be managed?
• Whole-class or group e-mails will be used in this school. Pupils will not have access to personal email accounts.
• Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
• Access in school to external e-mail accounts may be blocked.
• E-mail sent to external organisation should be written carefully and the sender should recognise the implication of sending such communication from a school address, in the same way as a letter written on school headed paper.
• The forwarding of chain letters is not permitted.

The School Website

How will published content be managed?
• The contact details on the school website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
• E-mail addresses should be published carefully, to avoid spam harvesting.
• The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
• The website should comply with the school's guidelines for publications, including respect for intellectual property rights and copyright.

Can pupils' images or work be published?
• Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Group photographs are more suitable than individual photographs.
• 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 of individual pupils are electronically published.
• Identified work can only be published with the permission of the pupil and parents.

Social Media

How will social networking and personal publishing be managed?
• Social networking sites will be blocked by the school's filtering system. Outside school:
• Pupils will be advised never to give out personal details of any kind that may identify them and/or their location.
• Pupils will be advised not to place any personal photographs on any social networking space.
• Teacher's official blogs or wikis should be password protected and run from the school website.
Teachers should be advised not to run social network spaces for students use on a personal basis.
• Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
• The school is aware that bullying can take place through social networking, especially when a space has been set up without a password and others are invited to see the bully's comments.

How will filtering be managed?
• The school's filtering system is set up and run by IT Connexions. They are responsible for managing this system, and if a site is found that is deemed inappropriate, it should be reported to them immediately.
• If staff or pupils discover unsuitable sites, the URL must be reported to the e-safety/ICT coordinator.   Any incidents will be logged and reported.

How can emerging technologies be managed?
• Emerging technologies will be examined by the e-safety/ICT co-ordinator/headteacher for educational benefit and a risk assessment will be carried out before use in school is allowed.
• Pupils will not be permitted to use mobile phones and other handheld technologies in school, with the exception of allowing their use by Year 6 pupils, on their school leaving day. Any telephonic communication with parents, should be made by the school, using the school land line.

How will internet access be authorised?
• The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
• All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.
• At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved online materials.
• Parents will be informed that pupils will be provided with supervised internet access.

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.
- 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.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will e-safety complaints be handled?
- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Complaints of a safeguarding nature must be dealt with in accordance with school safeguarding procedures.

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.
- Staff and volunteers will pay due regard to the Staff and Volunteer Acceptable Use policy Agreement.

Communications Policy

How will this policy be introduced to the pupils?
• E-safety rules will be displayed in all classrooms with Internet access.
• Pupils will be informed that network and Internet use will be monitored.
• An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
• Instruction in responsible and safe Internet use will precede Internet access.

How will this policy be discussed with staff?
• All staff will be given the school e-safety policy and its application and importance explained.
• Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
• Staff that monitor ICT use will be supervised by senior staff and have clear procedures for reporting issues.
• Staff training in safe and responsible internet use and on the school e-safety policy will be provided as required.

Caldew Lea Primary School

How will parents' support be enlisted?
• Parents' attention will be drawn to the school's e-safety policy in newsletters, the school brochure and on the school website.

Author/Owner	Date Written / Updated	Approved by Governors	Comments
	01-02-09		
	January 2010		Format standardised
AD		7 June 2011	Reviewed by C & P
KO and IJ	Dec 2015		Existing policy reviewed
KO/IJ	Jan 2016		Policy re-written from county model using attributed format