

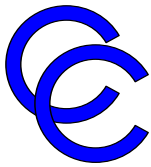
School Leader: Jane Brandon, Emma Luke

Link Governor:

Policy Approved	Signed: Jane Brandon	Date: May 2015
Policy Reviewed	Signed: Emma Luke	Date: Nov 2016
Policy Reviewed	Signed: Emma Luke	Date: Feb 2018
Policy Reviewed	Signed:	Date:
Policy Reviewed	Signed:	Date:

Contents

- 1. The Importance of internet and digital communications**
- 2. Roles and Responsibilities**
- 3. Teaching and Learning**
 - Benefits of the internet and digital communication in education
 - How the Internet and digital communications will enhance learning
 - Pupils will learn to evaluate Internet content
- 4. Managing Internet access**
 - Managing e-mail
 - Managing web-site content
 - Managing social networking and personal publishing
 - Managing filtering
 - Managing webcam and video conferencing
 - Managing emerging technologies
 - Authorising internet and email
 - Accessing the risks
- 5. Communicating the policy**
 - **Introducing the policy to pupils**
 - **E-safety policy and parents**
 - **E-safety policy and staff**
- 6. Maintaining ICT Security and Systems**
- 7. Handling Complaints regarding Internet Use**
- 8. Appendix 1**
 - Responsible Internet and Email Use - Parent/Carer Agreement
 - Letter to Parents - Responsible Internet Use
 - Staff Code of Conduct for Computing and Use of Digital Technology
 - References



1. The importance of Internet and digital communications

- The purpose of Internet and digital communication use in school are 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, digital media and digital communication use are part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for all pupils.
- The Internet and digital communications are an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide students with quality Internet and digital communications access as part of their learning experience.

2. Roles and Responsibilities

Governors

The role of the E-Safety Governor will include;

- Regular meetings with the E-safety officer
- Regular monitoring of E-Safety incident logs
- Reporting to relevant governors

Head teacher and Senior Leaders

- The Head teacher (E-Safety Officer) has a duty of care for ensuring the safety of members of the school community
- The SMT are aware of procedures to be followed in the event of a serious E-safety allegation being made against a member of staff.
- The Head teacher (E-safety officer) is responsible for ensuring that relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Officer.
- Receive reports of E-safety incidents and create a log of incidents to inform future E-safety developments

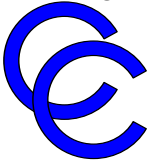
School Business Manager/Technical Staff

- Ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- Ensure that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- Liaise with school technical staff.
- That they keep up to date with E-safety technical information in order to effectively carry out their E-safety role and to inform and update others as relevant
- That the use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Head teacher for investigation and action.

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of E-safety matters and of the current E-safety policy and practices
- They have read, understood and signed the Staff Code of Conduct.
- They report any suspected misuse or problem to the E-Safety Officer for investigation and action

- All digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems



- E-safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the E-safety and acceptable use policies
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection/ Designated Safeguarding Officer

- Should be trained in E-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:
 - Sharing of personal data
 - Access to illegal/inappropriate materials
 - Inappropriate on-line contact with adults/strangers
 - Potential or actual incidents of grooming
 - Cyber-bullying

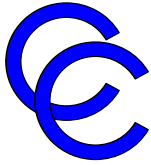
Pupils

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- Should understand the importance of adopting good E-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers

Some parents and carers have only a limited understanding of E-Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. Parents and carers will be encouraged to support the school in promoting good E-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Their children's personal devices in the school (where this is allowed)
- The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, and website. The school will also seek to provide information and awareness to parents and carers through:
 - Curriculum activities
 - Letters, newsletters
 - School notice boards
- The school website has direct links to Internet Service Providers' advice on how to set parental settings and to the Child Exploitation and Online Protection Centre (CEOP) website
- Parents/Carers evenings and events



3. Teaching and learning

Benefits of the internet and digital communication in education

Benefits of using the Internet in education include:

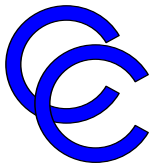
- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- exchange of curriculum and administration data with the LEA and DCFS.

How the Internet and digital communications will enhance learning

- 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 is acceptable and what is not acceptable 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 and retrieval.
- Pupils will be shown how to publish and present information to a wider audience.

Pupils will learn to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and by 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.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.
- Training will be made available to all staff in the evaluation of Web materials and methods of developing students' critical attitudes.
- Pupils will be taught how to report materials that they feel are distasteful, uncomfortable and unpleasant or threatening to an adult or using the CEOP report abuse icon.



4. Managing internet access

Managing e-mail

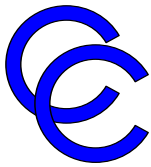
- Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication.
- Pupil accounts will be restricted as appropriate.
- Pupils will be taught the importance of keeping their passwords private.

Managing web site content

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be identified.
- Pupil image file names will not refer to the pupil by name.
- Pupils' full names will not be used anywhere on the Web site, particularly associated with photographs.
- Written permission from parents will be sought before photographs of pupils are published on the school Web site.
- The head teacher or nominee will take overall editorial responsibility and ensure content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications. The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Managing social networking and personal publishing

- Pupils will not be allowed access to public or unregulated chat rooms.
- Children should use only regulated educational chat environments. This use will always be supervised and the importance of chat room safety emphasised.
- Newsgroups will not be made available unless an educational requirement for their use has been demonstrated.
- Pupils will be advised not to give out any personal information that could identify themselves, their school or their friends.
- Pupils will be advised on the use of avatars and nicknames when using any kind of chat or social networking site.
- Parents and pupils will be advised of dangers that social network spaces outside of school bring and how to stay safe.



Managing filtering

- The school will work in partnership with parents, the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate and effective.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (see appendix).
- If staff or students require an alternative filtering strategy, an assessment will be made and a new filtering profile designed, where appropriate.

Managing webcam and videoconferencing

- Use of webcams and videoconferencing must be supervised.
- Appropriate permissions must be obtained.

Managing emerging technologies

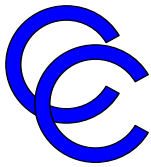
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- School leaders need to have an awareness that new mobile wireless internet technology could bypass school filtering and leave pupils open to inappropriate content.

Authorising Internet, and email access

- The school will keep a record of all staff and pupils with email accounts. The record will be kept up-to-date, for instance a member of staff leaving or the withdrawal of a pupil's access.
- Pupils will be taught not to share their password with others.
- In EYFS and Key Stage 1, access to the Internet will be by adult demonstration with supervised access to specific, approved on-line materials.

Assessing the risks

- 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 LA 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 Internet policy is implemented and compliance with the policy monitored.

5. Communicating the policy

Introducing the policy to pupils

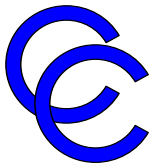
- Rules for Internet access will be posted near all computer systems.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- Safe and responsible use of technology will be embedded in the PSHE curriculum.
- E-safety will be included as part of the scheme of work for Computing.

E-safety policy and parents

- Parents' attention will be drawn to the School Internet Policy in newsletters, the school brochure and on the school web site.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- A stock of relevant leaflets from organisations such as BECTA, PIN, and NCH Action for Children will be maintained.

The e-safety policy and staff

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
- All staff including teachers, supply staff, classroom assistants and support staff, must read and sign the Staff Code of Conduct for Computing and Use of Digital Technology.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.

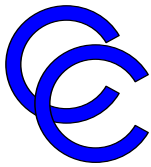


6. Maintaining ICT system security

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the LA, particularly where a wide area network connection is being planned.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Use of disks and other portable data storage devices will be reviewed. Personal portable data storage devices may not be brought into school and used without specific permission and 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 will be regularly checked.
- The IT co-ordinator / network manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

Handling complaints regarding Internet use

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions may need to be applied. These include: - interview/counselling by head teacher; - informing parents or carers; - removal of Internet or computer access for a period, which could prevent access to school work held on the system.



Guidelines on the use of technologies in school.

Communication Technologies	Staff				Pupils			
	allowed	allowed at certain times	allowed with SLT permission	Not allowed	allowed	allowed at certain times	allowed with SLT permission	Not allowed
Mobile phones may be brought to school	√							√
Mobile phones may be in the cupboard on silent or vibrate	√							√
Personal use of mobile phones during lesson time				√				√
Taking photos on mobile phones or personal cameras				√				√
Use of school mobile devises. E.g. cameras and tablets	√					√		

Appendix 1

Responsible Internet and Email Use

Parent/carer consent for web publication of work and photographs.

I agree that, if selected, my children's work may be published on the;
School website **yes/no** (delete as appropriate)

I also agree that photographs that include my child may be published subject to the school rules that
photographs will not clearly identify individuals and that full names will not be used.

School website **yes/no** (delete as appropriate)

Names Child _____

Name: _____ (parent/guardian)

Signed: _____ Date: _____

Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of computing skills, our school is providing supervised access to the Internet.

We believe that the use of the Web and email is worthwhile and an essential tool for children as they grow up in the modern world.

Please read the rules and agreements for responsible Internet and email use. Then sign and return the agreement.

Also please read and if you agree sign the web publication consent for photographs and work.

Although there have been concerns about pupils having access to undesirable materials, we are taking positive steps to deal with this risk in school. Our school Internet access provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home and we enclose references to information on safe Internet access that may be of use.

Whilst every effort is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet.

The School will not be liable under any circumstances for any damages arising from your child's use of the Internet facilities.

I enclose a copy of the rules for Responsible Internet Use that we operate at our school.

We also have a number of leaflets from national bodies that explain issues further.

Should you wish to discuss any aspect of Internet use please telephone the office to arrange an appointment.

Yours sincerely

A J Brandon
Head teacher

STAFF CODE OF CONDUCT FOR COMPUTING AND USE OF DIGITAL TECHNOLOGY.

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff, governors, volunteers and students are aware of their professional responsibilities when using any form of ICT.

All staff, governors, student and volunteers are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with the E-Safety Officer.

- I will only use the school's email/Internet /Website and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the computing system security and not disclose any passwords or codes provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number or personal email address, to pupils or parents (unless prior permission given by SLT for school trips.)
- I will ensure that I am not in contact with any pupils and parents at Cavendish Close Infant School on Social Networking sites including Facebook and Twitter.
- I will only use the approved, secure school email system for any school business.
- I will ensure that any pupil or personal data is kept securely on an encrypted device and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will only install hardware or software on a school laptop for educational purposes.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils will only be taken on school devices.
- My personal mobile phone will only be used during lunch breaks and will be kept on silent and in a cupboard at all times during the school day.
- Images of pupils will only be stored on the school network or school encrypted devices.
- Parental consent is required to publish any images on the school website or distributed outside school.
- I understand that my use of the Internet on school devices, eg laptops, i-pads etc. and other related technologies can be monitored by the Head teacher.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the E-Safety Coordinator.
- I will not disclose information about Cavendish Close Infant School on social media.

- I will uphold public trust by maintaining high standards of ethics and behaviour within and outside school as stated in teachers' Standards.
- I will support and promote the school's E-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I agree to follow this code of conduct and to support the safe use of computing and digital technology throughout the school.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete 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.

Signed: _____

Name: _____

Date: _____

References

Particularly for Parents

National Action for Children (NCH)

Parents' Guide on Internet usage www.nchafc.org.uk/itok/itokhome.html

Current activities to promote safe use www.nchafc.org.uk/internet

Internet Watch Foundation - report inappropriate Web sites www.iwf.org.uk Safe Surfing Guide for parents and carers: www.iwf.org.uk/safe/ which article on Internet filtering for home use www.iwf.org.uk/safe/which/total.htm

Parents Information Network (PIN) www.pin.org.uk/learning/safeindx.htm Comprehensive guidelines on Internet safety

Recreational Software Advisory Council (RSACi) www.rsac.org/ Promotes rating systems for Web sites, and is a third party rating bureau

Particularly for Schools

Associations of Co-ordinators of IT (ACITT) <http://atschool.eduweb.co.uk/acitt/aup.html>

Acceptable use policy for the Internet in UK Schools

BECTa www.becta.org.uk/technology/infosheets/html/accuse.html

Advice and guidance on appropriate computer use

British Computer Society www.bcs.org.uk/iap.html A guide for schools prepared by the BCS Schools Committee and the National Association of Advisers for Computer Education (NAACE)

DfEE Superhighway Safety <http://safety.ngfl.gov.uk>

Essential reading. For free pack telephone: 0845 6022260 **Internet Watch Foundation** - www.iwf.org.uk Invites users to report illegal Web sites

Scottish Education Department www.scotland.gov.uk/clickthinking Comprehensive safety advice

SEGfL ICT Security Policy www.segfl.org.uk/ An overview of the security of networks with Internet access. **Copyright** www.templetons.com/brad/copymyths.html Covers the main aspects of copyright of digital materials, US-based but relevant.

Internet Users Guide www.terena.nl/libr/gnrt/ A guide to network resource tools, a book (ISBN 0-201-61905-9) or free on the W

Policy Change History Sheet

Policy title: E-Safety		
This policy was written May 2015		
Review Date	Section	Summary of change
30.11.16	Contents (p.1)	School Leader, staff change to Emma Luke
	Contents (p.1)	Addition of titles in Appendix 1
	E-Safety Policy and Staff (p.7)	Reduced to four bullet points. Bullet point 5 omitted. Bullet point 2 amended.

	Guidelines on the use of technologies in School (p.9)	Update – staff mobile phones may be on the desk on silent or vibrate.
	Staff Code of Conduct (p.12)	Bullet point 5 - will include parents. Bullet point 11 – new addition, protocol for staff mobile phones. Updates made by Emma Luke.