



E Safety Policy

Rationale

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and rules to guide staff, pupils and visitors in their online experiences.

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff, pupils and families;
- A comprehensive, agreed and implemented e-safety policy;
- Secure, filtered broadband;
- A school network that complies with the National Education Network standards and specifications.

The school's e-safety policy will operate in conjunction with other policies including those for Positive Behaviour, Anti-Bullying, Health & Safety, Data Protection, Child Protection & Safeguarding.

For further Information

Chat Danger	www.chatdanger.com
Child Exploitation and Online Protection Centre	www.ceop.gov.uk
Childnet	www.childnet-int.org
Hector's World	www.hectorsworld.com/island/index.html#HOMEPAGE
Cyber Café	www.thinkuknow.co.uk/8_10/cybercafe/Cyber-Cafe-Base/
Digizen	www.digizen.org
Kidsmart	www.kidsmart.org.uk/
Think U Know	www.thinkuknow.co.uk
YHGfL eSafeguarding	www.yhgfl.net/esafeguarding/esafety

Aims

- To educate staff and children about the benefits and risk of using new technologies both within and outside of school.
- To provide safeguards and agreement for acceptable use to guide all users, staff and children in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the boundaries of our school.
- To develop links with families and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Teaching & learning

- The purpose of Internet use 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 a part of the statutory curriculum and a necessary tool for staff and pupils.
- 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;
- educational and cultural exchanges between pupils world-wide through the video-conferencing;
- 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 with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with DfES;
- access to learning wherever and whenever convenient.

Broad Guidelines

The Internet enhancing learning

- 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.
- 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:
- All staff and volunteers will be asked to follow an e-safety code of conduct and to sign to agree to the LA's Use of internet and email policy.
- Children will be introduced and asked to follow a code of conduct. This will be displayed in classrooms.

There are many potential risks for children and young people including:

- Accessing age inappropriate or illegal websites.
- Receiving unwanted or upsetting text or e-mail messages or images.
- Being "groomed" by an adult with a view to meeting the child or young person for their own illegal purposes including sex, drugs, or crime.
- Viewing or receiving socially unacceptable material such as inciting hatred or violence.
- Sending bullying messages or posting malicious details about others.
- Ignoring copyright law by downloading music, video or even homework cheat material.

Cause for concern - a child who:

- Is becoming secretive about where they are going to or who they are meeting.
- Will not let you see what they are accessing online.

- Using a webcam in a closed area, away from other people.
- Accessing the web or using a mobile or PDA (Personal Data Assistant) for long periods and at all hours.
- Clears the computer history every time they use it.
- Receives unexpected money or gifts from people you don't know.

Cause for concern - an adult who:

- Befriends a child/children or young person/people on the internet or by text messaging.
- Has links to children or young people on their Facebook or other social network site.
- Is secretive about what they are doing and who they are meeting.

Any concerns should be reported to the Headteacher or Deputy Head (Designated Safeguarding Lead) immediately.

Minimising risk:

Talk and teach the children to children about what they are accessing on line.

- Keep the computer/s in a general space where we can monitor what is going on.
- Explain the risks of giving out personal details online.
- Talk about how people can be anyone they want to be online: by using misleading emails, photographs of other people, telling lies about their age, school, hobbies.
- Encourage children and young people to think carefully about which photographs or videos they use on line this material can be used and tampered with by other people, or they may not be appropriate.
- Advise children and young people to only text, chat or webcam to people they know for real.
- Discuss how people hide their identities online and the importance of never meeting new online "friends" for real.
- Make sure children and young people understand they can talk to us or their parents and/or carers about anything that makes them feel uncomfortable.
- Look on the internet together for information about how to deal with, or report, problems.
- Talk about how, when information or images get onto the net, they can never be erased or retrieved.
- Training/information for Staff and families on E-safety.

Evaluating Internet Content

If staff or children discover unsuitable sites, the URL (address), time, date and content must be reported to the Internet Service Provider via the Headteacher. Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

The evaluation of on-line materials is a part of every subject.

Managing Internet Access

- The security of the school ICT systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Calderdale IT support will review system capacity regularly.

Published Content - Website

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- Leadership & Management will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

- Photographs that include pupils will be selected carefully and written consent will be sought by families when children start school.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.

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 the school day. The sending of abusive or inappropriate text messages is forbidden.

E-safety complaints

- Complaints of children's internet misuse will be dealt with by the Headteacher or Deputy Head.
- Any complaint about staff misuse must be reported to the Head teacher.

Employees

- All staff must accept the terms of the LA Internet and Email Usage Policy before using any Internet resource in school. (APPENDIX 1)
- All staff will be given the E-Safety Policy as part of their induction. The policy will also be available on the school website.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff development in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

It is the duty of families to ensure that their child/children remain safe outside of school when using the internet and other electrical devices.

Written/amended: February 2017

Next review date: February 2020

Policy on Staff Internet and E-Mail Usage

This policy applies to all LA employees including those of Central Street Infant & Nursery School.

“Employees” includes all employees of the Council as well as contractors, temporary staff and third parties provided with access to the Council’s information assets.

The Internet is an unregulated environment. Although the LA has implemented pro-active filtering they will not be liable for any material viewed or downloaded.

This policy is neither exclusive nor exhaustive; if you are in any doubt about whether you should be using the facilities for a particular purpose – consult the Headteacher.

Failure to comply with this policy may constitute gross misconduct and could lead to dismissal.

Suspected illegal activities may also be reported to the Police.

RED – Unacceptable Use

- DO NOT knowingly, view, send or receive material, which is obscene, sexually explicit, offensive, defamatory, racist or homophobic in nature, or which is intended to cause the receiver or anyone who sees the material harassment, alarm or distress.
- DO NOT use the Internet and e-mail facilities for personal purposes in works time, UNLESS usage is in compliance with the Green – Acceptable Use section below.
- DO NOT use e-mail to engage in gossip.
- DO NOT make libellous statements about individuals or other organisations.
- DO NOT make statements purporting to represent the school when they are personal views.
- DO NOT make derogatory remarks or express derogatory opinions regarding the Council.
- DO NOT knowingly, infringe copyright or intellectual property rights.
- DO NOT knowingly, use the facilities for any activity, which is illegal or fraudulent.
- DO NOT use the facility to pursue personal business interests, for gambling or for political purposes not directly related to your job.
- DO NOT allow anyone else to use your Internet access or e-mail account or provide any other person with the means to access these facilities e.g. By disclosing your user ID and password etc.
- DO NOT knowingly engage in any activity which threatens the integrity or availability of the school's systems.
- DO NOT attempt to gain unauthorised access to (hack) any server/facility whether inside or outside the school/LA.
- DO NOT Install any unauthorised programs, such as screen savers, on the schools information assets.

GREEN – Acceptable Use







- YOU MAY use the Internet and e-mail facilities for work purposes.
- YOU MAY use the Internet and e-mail facilities for personal purposes outside works time.
- YOU MAY open personal e-mails received in your school e-mail account in works time.
- YOU MAY use the facilities, with the prior approval of the SLT/governors, for personal purposes in works time.

If your specific circumstances require a dispensation from this Policy, written permission should be sought from the governing body.

E-Safety

Think then Click

These rules will help us to stay safe on the Internet:

	We only use the internet when an adult is with us
	We can click on the buttons or links when we know what they do.
	We can search sites chosen by an adult.
	We always ask if we get lost on the Internet.
	Messages we send will be polite, sensible and should not contain any personal information.
	We always tell an adult if we see anything that makes us unhappy or uncomfortable.