E-SAFETY POLICY

The importance of ICT

The increasing use of technology in all aspects of society makes confident, creative and productive use of ICT an essential skill for life. ICT capability encompasses not only the mastery of technical skills and techniques, but also the understanding to apply these skills purposefully, safely and responsibly in learning, everyday life and employment. ICT capability is fundamental to participation and engagement in modern society. ICT can be used to find, develop, analyse and present information, as well as to model situations and solve problems. ICT enables rapid access to ideas and experiences from a wide range of people, communities and cultures, and allows pupils to collaborate and exchange information on a wide scale. ICT acts as a powerful force for change in society and citizens should have an understanding of the social, ethical, legal and economic implications of its use, including how to use ICT safely and responsibly. Increased capability in the use of ICT supports initiative and independent learning, as pupils are able to make informed judgements about when and where to use ICT to enhance their learning and the quality of their work.

E-Safety

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. (Though children are not encouraged to use social media sites such as Facebook and Twitter, these issues will be discussed so children can become responsible digital citizens when they are older. It is also recognised that many of our pupils are already active on social media networks, despite not meeting age criteria.)

The school's e-safety policy will operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data Protection, mobile phones and Security.

E-Safety depends on effective practice at a number of levels:
• Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
• Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
• Safe and secure broadband Network including the effective
Management of content filtering.

1. Policy Creation

The school will appoint an e-Safety Coordinator. This may be the ICT Co-ordinator, supported by the Designated Child Protection Coordinator as the roles overlap.

It has been agreed by the senior management, staff and governors. The e-Safety Policy and its implementation will be reviewed annually**.**

2. Teaching and learning

2.1 The importance of Internet use:

- 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.

- Internet access is available for all students providing they show a responsible and mature approach to its use. It can be withdrawn if misused.
- 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, security and reputation.
- Pupils will be given lessons about internet safety and cyberbullying so they know how to respond safely to any incidents that they come across.

2.2 Benefits of the Internet to education include:

- Access to world-wide educational resources including museums and art galleries;
- Access to relevant up to date information and data;
- 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 calderdale lea and dfes;

2.3 Using the Internet to 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 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.
- Pupils will be given opportunities to use the Internet independently but under supervision.

2.4 Evaluation of Internet content

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will 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 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 but is taught specifically in some ICT lessons.

3. Managing Information Systems

3.1 Information system security

- Security strategies will be discussed with the Calderdale ICT Support team regularly.
- The schools server will be backed up to an offsite location daily.
- Anti-Virus protection will be updated regularly.
- The security of individual staff and pupil accounts will be reviewed regularly.
- The administrator account password will be changed immediately if it becomes known.
- Computers (including mobile devices) may not be connected to the school network both physically or wirelessly without specific permission
- Personal data will not be sent over the Internet unless it is essential. Any personal data sent over the Internet will be encrypted or otherwise secured.
- Portable media may not used without specific permission.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail as these pose a virus threat.
- Personal data will not be stored on school servers without specific permission. Files held on the school's network will be regularly checked.
- Software will not be installed/removed from computers without specific permission.
- The ICT co-ordinator / network manager will review system capacity regularly.
- Security, including data encryption will be discussed regularly with the ICT technician and Schools ICT
- Laptops and other digital storage that is likely to be taken off site and that may contain sensitive data will be encrypted.

3.2 E-mail

- Pupils may only use approved e-mail accounts from within school.
- Pupils must immediately tell a teacher if they receive offensive e-mail or other electronic message (SMS, MMS, in game messaging etc).
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission. This will be taught and explained annually in e-safety lessons.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations in the school's name should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- All staff will use a professional …@Luddenden-CE.calderdale.sch.uk e-mail account for work related communications.
- Any email addresses held by the school (Parent/carer/staff/children/group) will be stored securely and not shared with any outside agencies without permission.

3.3 Management of published content

- The contact details on the website should be the school address, office e-mail and telephone number. Staff or pupils' personal information must not be published.
- The head teacher or the ICT co-ordinator will take overall editorial responsibility for published material in public areas on the school website 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.

3.4 Publishing of pupil images

- Written permission from parents or carers will be obtained before images of pupils are electronically published by the school. This will take the form of a written form signed when a pupil joins the school.
- Pupils' full names will not be used in any public area of the website, particularly in association with photographs.
- Written permission from the school should be obtained before pupils or parents/carers publish images taken from the school website or of school events. Any images parents take or obtain of any child in the school other than their own child/children should be for personal use and not shared or published electronically, including on social media networks such as Twitter and Facebook.
- Work can only be published with the permission of the pupil and parents.
- Children will not be permitted to publish images of themselves or other children at school events. This also includes the use of images on Facebook or other social networking sites.

3.5 Management of social networking and personal publishing

Examples include: Facebook, Twitter, blogs, wikis, MySpace, Bebo, Piczo, Windows Live Spaces, MSN space, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be reminded about using social networking sites that are age restricted at a higher age than their own. Though the school cannot stop this use outside of school, advice will be given to staff, pupils and parents about the potential risks of such sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Staff will be informed of the risks associated with the use of social networking sites.
- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Anything published on the internet should be considered public regardless of how secure the website is. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- Teachers' official blogs or wikis should be password protected. Teachers should be advised not to run social network spaces for student use on a personal basis.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to **all** others.
- Students should be advised not to publish specific and detailed private thoughts unless they would consider them to be public.
- Luddenden School is 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. When an incident is brought to the school's attention, website administration will be alerted and informed where necessary.

3.5 Web Filtering

- The school will work with Calderdale ICT to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Coordinator and Calderdale ICT.

- 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 (addresses later).
- When web filtering is reduced by using the Cal-Unf code, children may not use the teacher's laptop or other machine that has de-restricted internet access.

3.7 Video conferencing (currently not applicable – review if equipment is purchased)

Possible statements

The equipment and network

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses should not be made available to other sites.
- Videoconferencing contact information should not be put on the school Website.
- The equipment must be secure and if necessary locked away when not in use.
- School videoconferencing equipment should not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled.

Users

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing should be supervised appropriately for the pupils' age.
- Parents and guardians should agree for their children to take part in videoconferences, probably in the annual return.
- Responsibility for the use of the videoconferencing equipment outside school time needs to be established with care.
- Only key administrators should be given access to the videoconferencing system, web or other remote control page available on larger systems.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.
- Recorded material shall be stored securely.
- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

3.8 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, unless as part of a learning experience. The sending of abusive or inappropriate text messages is forbidden. Any such use will be subject to the school's behaviour policy and dealt with by the head teacher – See mobile phone policy.
- Children will not be permitted to store mobile phones or other portable devices except in the school office. Mobile phones networks will not be used by children on school premises.
- Staff will be issued with a school phone where contact with pupils is required whilst off site. Staff will never contact pupils using their own personal mobile, landline or other device.

3.9 Protection of personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4 Policy Decisions

4.1 Authorisation to use the Internet

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- Parents will be asked to sign and return a consent form for pupil access when pupils join the school.

4.2 Risk Assessment

- 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. Neither the school nor Calderdale LEA can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school should 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.

4.3 E-safety complaints procedure

(See also **Response to an incident of concern**, **appendix 1)**

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher. Head teacher misuse will be reported to the Governors or Deputy Head
- Pupils and parents will be informed of the school complaints procedure if necessary.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Discussions will be held with the Schools Police Liaisons Officer to establish procedures for handling potentially illegal issues.
- If the well being of a child is compromised, the Child safety officer will be informed. Parents will be informed immediately unless this could affect the well being of a child.
- Sanctions within the school discipline policy include:
  - interview/counselling by the head of year;

- informing parents or carers;
- removal of Internet or computer access for a period.

4.4 Community use

- 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.

5 Communications Policy

5.1 Policy introduction

- E-Safety rules will be posted in rooms with Internet access.
- Pupils will be informed that network use and Internet use will be monitored.
- An e-safety training programme will be taught each school year, appropriate to the age group, to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede Internet access.

5.2 Staff sharing of e-safety policy

- The ICT policy will be shared and its application and importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management 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.

5.3 Parental involvement

- Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations listed in section 6 e-Safety Contacts and References.

To be read in conjunction with:

- Mobile phone policy
- Child protection policy
- Acceptable use policy
- ICT policy
- Data and security procedures

6 E-Safety Contacts and References

BBC Chat Guide
http://www.bbc.co.uk/chatguide/

Becta
http://www.becta.org.uk/schools/esafety

Childline
http://www.childline.org.uk/

Childnet

http://www.childnet-int.org

Kidsmart

http://www.kidsmart.org.uk

Digizen

http://www.digizen.org/cyberbullying/film.aspx

Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk

e-Safety in Schools
http://www.clusterweb.org.uk?esafety

Grid Club and the Cyber Cafe
http://www.gridclub.com

Internet Watch Foundation
http://www.iwf.org.uk/

Internet Safety Zone
http://www.internetsafetyzone.com/

West Sussex e-Safety Pages
http://wsgfl.westsussex.gov.uk/ccm/navigation/learners/stay-safe/bullying/e-safety-in-west-sussex-schools/

Kidsmart
http://www.kidsmart.org.uk/

NCH – The Children's Charity
http://www.nch.org.uk/information/index.php?i=209

NSPCC
http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm

Stop Text Bully
www.stoptextbully.com

Think U Know website
http://www.thinkuknow.co.uk/

Virtual Global Taskforce – Report Abuse
http://www.virtualglobaltaskforce.com/

Appendix 1

Response to an Incident of Concern

The screening tool is available on the Children's