Introduction

"All agencies providing services to children have a duty to understand e-Safety issues, recognising their role in helping children to remain safe online while also supporting adults who care for children".– Becta 2008 – Safeguarding Children in a Digital World

Effective Practice in e-Safety

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

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

PIES Model for Limiting e-Safety Risks

- Policies and Practice
- Infrastructure and Technology
- Education and Training
- Standards and Inspection

Principles of e-Safety (April 2012)

Technology enhances learning, and schools and colleges can do much to ensure students get the most from it, by encouraging responsible online behaviour. Involving children and young people in the development of their school's e-Safety policy can minimise risk and embed important principles such as

- Keep personal information private
- Consider the long-term implications of any content posted online
- Do not upload or post inappropriate, offensive or illegal content to their own or other online spaces
- Read and adhere to any website's terms of conditions of use – including those around age restrictions.
- Many search engines provide filtering facilities to remove unsuitable sites and advertising for search results, and most web browsers allow users to customise and adjust their settings for security, privacy and content. There are also a number of search engines which are suitable for children and young people.

Social Networking is becoming increasingly popular in schools to support learning and encourage creative use of the internet, and publish and share content. These technologies need to be used in a safe and responsible way, and appropriate online behaviour encouraged.

Staff and helpers can also be susceptible to risks from social networking. Schools should take appropriate steps to help staff and helpers maintain a professional level of conduct in their use of technology and online behaviour.

More information can be obtained from the following website http://bit.ly/12x5bZi

At Ludlow Junior School we have a policy in place which considers the following issues:

- The acceptable use of ICT by all users.
- e-Safety procedures, e.g. incidents of misuse of ICT by users, safeguarding incident when a user is at risk of or has come to actual harm through the use of ICT.
- e-Safety training for staff and pupils.
- The technology available to users, its features and settings, e.g. virus protection, filtering and monitoring.
- A named person with responsibility for e-Safety which should ideally be a member of the Senior Management Team and is not necessarily the ICT Co-Ordinator, as e-Safety is primarily about safeguarding and not the technology itself.
- That regular training is in place for all aspects of e-Safety.

For Ludlow Junior School the named person with overall responsibility for e-Safety is the Executive Headteacher.

Delegated responsibility for website content, internet infrastructure, filtering and data procedures falls to those staff with web training.

The term 'Staff' is used as a broad term within this policy and includes every adult who works on the school site as well as volunteers and governors.

Ludlow Junior School's e-Safety Policy will cover the safe use of internet and electronic communications technologies such as mobile phones and wireless connectivity. The policy will highlight the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

e-Safety Risks and Issues

e-Safety risks and issues can be roughly classified into three areas: content, contact and commerce. The following are basic examples of the types of e-Safety risks and issues that could fall under each category.

Content:

- Exposure to age-inappropriate material.
- Exposure to inaccurate or misleading information.

- Exposure to socially unacceptable material such as that inciting violence, hate or intolerance.
- Exposure to illegal material, such as images of child abuse.
- Downloading of copyrighted materials, e.g. music and films.
- Plagiarism.

Contact:

- Grooming using ICT, leading to sexual assault and/or child prostitution.
- Bullies using ICT (email, mobile phones, chat rooms etc.) as a way to torment their victims.
- Children and young people self-publishing information - sometimes inappropriate – about themselves and therefore putting themselves at risk.
- Commerce:
- Exposure to inappropriate commercial advertising.
- Exposure to online gambling services.
- Commercial and financial scams.

Infrastructure & Technology

Becta recommends that all organisations providing services to children and young people use an accredited service supplier to deliver filtered internet access, configured to their own local circumstances and requirements.

Under the accreditation scheme, a product for filtering internet content must meet or exceed the following requirements:

- There must be telephone and web-based support for all aspects of the service.
- The product must block 100 per cent of illegal material identified by the Internet Watch Foundation (IWF) Child Abuse Images and Content (CAIC) URL List.
- The product must be capable of blocking 90% of inappropriate content in each of the following categories:

- Pornographic, adult, tasteless or offensive material
- Violence (including weapons and bombs)
- Racist, extremist and hate material
- Illegal drug taking and promotion
- Criminal skills and software piracy

- It must be possible to request (or make) amendments to the blocked content.

Firewall and virus protection is provided by Exponential-e for computers connected to the schools network. It is the schools responsibility to ensure that the virus definition files are updated regularly on all school machines to maintain protection. Monitoring Systems – to keep track of who downloaded what, when and on which computer.

Managing Filtering
All Ludlow junior School staff will work with the *ICT Technician* to ensure systems to protect pupils are reviewed and improved. If staff or pupils come across unsuitable online materials, the site must be reported to the *Executive Headteacher*. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

The current filtering system is designed with various levels of filtering dependent on the accessing user. When logged in as teaching member of staff, the user will have a wider variety of access option but still filter to requirements of an educational environment. When logged in as a pupil, the user will have a greater restriction on accessible content thus co-operating with e-Safety requirements. To ensure that filtering is adhered to each user is supplied with an individual login that is kept secure with regular password changes. Users are informed that they are not to share logins as they will be held accountable for content accessed.

Teaching and Learning

Why the Internet and Digital Communications are Important.
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. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet Use 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 Internet use is acceptable and what is not and given clear objectives for Internet use. 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 shown how to publish and present information to a wider audience.

Pupils Will Be Taught How to Evaluate Internet Content
The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught the importance of cross-checking information before accepting its accuracy. Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon, Hector Protector or the schools e-Safety officer.

Managing Internet Access
Information System Security
School ICT systems security will be reviewed regularly. Virus protection will be updated regularly. Security strategies will be discussed with the Local Authority.
Users and Logins

Each user is supplied with an individual login and password (this includes staff, pupils and visitors with access to computer systems). Before a user is allowed to access any networked computers within the school environment the procedures must be carried out to ensure they understand the policy and the acceptable use of computer systems within school.

For Staff
Staff must be sent to the *ICT Technician*. Once there they will discuss the Staff Code of Conduct and sign the document to confirm they understand the rules for usage. They will then be provisioned with their required access to the system with a unique username and password (for all required systems e.g. SIMs, email and domain login etc.). They must ensure they do not share their logins with any other users. If this occurs then the school reserves the right to remove access to any systems in place.

For Pupils
Pupils are supplied with individual logins and passwords when joining or at the beginning of the year. An email address may be provisioned later on. Passwords and logins must be kept private and pupils must be educated on the importance of this. Please see the below information on individual logins. A computer access form is provided in school signup packs and these are kept on file. A pupil will not be allowed access to any networked systems without the required confirmation.

For Visitors/Students and Other Users
There will be individual logins available to the above listed users which will be designated at time of arrival. This will ensure that we are able to track and maintain coverage within the required school policies and to ensure correct coverage of the e-Safety Policy and the Staff Code of Conduct which applies to all adult visitors who will require access to domain systems.

Logins and Passwords
Within the Lightspeed Systems Rocket there is a function to recognise a logged in user and the system they are logged into. This will track the user to ensure that there are no inappropriate instances of internet usage. The system will log all of the required information.

Internet Code of Conduct
Pupils should be supervised at all times when using the Internet. Independent pupil use of telecommunications and electronic information resources is not permitted at Ludlow Junior School. Access to school systems must be with a unique username and password, which must not be made available to any other staff member or pupil.

All Internet activity should be appropriate to staff's professional activity or the student's education.

Staff may use their Internet facilities for non-business research or browsing during meal time breaks or outside of work hours, provided that all other Internet usage policies are adhered to.

Internet activity that threatens the integrity or security of the school's ICT systems or activity that attacks, corrupts, or threatens the security of other organisations' systems is prohibited.

Copyrights, software licensing rules, laws of the land, property rights, privacy and the rights of others must be respected and adhered to at all times.

The Internet must not be used to access, display, store, transmit, distribute, edit or record inappropriate sites such as those containing pornographic, violent, racist, discriminatory, criminal skills related, illegal drugs related or offensive material. Users will recognise materials that are inappropriate and, if deliberately accessing them, should expect to have their access removed.

The Internet must not be used to download entertainment software or games, or play games against other Internet users, unless for educational purposes.

Uploading materials or files to City Council systems must only be performed on machines that have virus protection to the latest corporate standards and with appropriate authorisation from the relevant departments.

Downloading of files to school systems using ftp, email and http must be carried out with an appropriate level of care and thought.

Users must not download or install software on any systems unless directed to do so by the school *ICT Technician*.

The Internet must not be used to engage in any activity for personal gain or personal business transactions.

The Internet must not be used to conduct or host any on-going non-education related activities, including discussion groups, chat lines, newsgroups or any other form of online club.

The Internet must not be used for personal or commercial advertisements, solicitations or promotions.

The use of a computer system without permission or for a purpose not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.

To ensure compliance with the acceptable use policy for Web browsing and email the school reserves the right to monitor and record activity in these areas. All users should

therefore have no expectation of privacy in respect of their web browsing and email activities when using the school's computer facilities.

Email Code of Conduct

 Access to email should only be via the authorised user name and password, which must not be made available to any other staff member or pupil.

 In relation to any form of school communication all emails must be sent through the recognised email system. Currently the recognised method is *Office365*.

 Pupils/Staff may only use approved e-mail accounts on the school system.

 Pupils/Staff must immediately inform the *Teacher/ICT Technician* if they receive offensive e-mail.

 In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

 Normally, access to another staff user's email account will not be granted to anyone. However, there are occasions when such access may be legitimately needed, e.g. To aid investigation of suspected irregularities; upon summary dismissal of an employee; during suspension or prolonged absence of an employee; where the retrieval of information is necessary to allow continuation of work in hand by the user whose ID/password combination is to be circumvented.

 Attachments from unknown sources should not be opened, but deleted immediately. All attachments should be scanned for viruses.

 Schools are responsible for all email sent and for contacts made that may result in email being received.

 Pupils must not send or publish their personal details in an email to an unknown recipient

 Posting anonymous messages and creating or forwarding chain letters is forbidden.

 As email can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.

 Messages that contain abusive or objectionable language, that libel others, or that infringe the privacy rights of others are forbidden.

 Changes must not be made to other people's messages that are then sent on to others without making it clear where the changes have been made.

 Users must not pretend that they are someone else when sending email, or use someone else's account to send a message.

 Users must not publish, electronically or otherwise, any school email address as a point of contact for non-education related activities.

 Personal or otherwise sensitive data must not be transferred via email unless the security of the data whilst in transit can be assured.

Social Networks, Chat Rooms, Instant and Text Messaging Code of Conduct
The school will control access to social networking sites, and consider how to educate pupils in their safe use. Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location. Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
 The use of such websites should only be permitted within an educational or professional context.

 Pupils should be supervised at all times when using such websites.

 Pupils should be taught to understand the importance of personal safety on the Internet, i.e. taught never to give out personal contact information or to arrange to meet someone they have met online.

 Access to internet related services such as instant messaging, chat services and social networks is commonplace outside of the school environment. Many young people own, or have access to a mobile phone which increasingly are providing online access. For this reason, schools will need to ensure that pupils are taught safe and responsible behaviours whenever using ICT.

 All staff should be aware of the Ludlow Junior School guidelines for the use of social networking sites. The guidelines are in place to protect staff, volunteers and governors from allegations of professional misconduct in their use of networking sites at all times in connection with school matters (please see attached Social Networking Policy).

Please refer to the *Social Networking Policy* for further details and information (

Community use of the Internet
The school will liaise with local organisations to establish a common approach to e-Safety.

Assessing Risks
The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school cannot accept liability for any material

accessed, or any consequences of Internet access. 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 and effective.

Handling e-Safety complaints
Complaints of Internet misuse will be dealt with by the *Executive Headteacher*. Any complaint about staff misuse must be referred to the *Executive Headteacher*, who may then consult LADO or HR. Complaints of a child protection nature must be dealt with in accordance with the Ludlow Junior School child protection procedures. Pupils and parents will be informed of the complaints procedure (see schools complaints policy). Pupils and parents will be informed of consequences for pupils misusing the Internet.

Policy Decisions
Authorising Access to Ludlow Junior School ICT Systems
 All staff/placement students/visitors must read and sign the Staff Code of Conduct for ICT before using any school ICT resource, this includes volunteers and governors.

 The school will maintain a current record of all users who are granted access to school ICT systems.

Introducing the e-Safety Policy to Pupils
 All pupils must read and sign the e-Safety contract before using any school ICT resource.

 e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.

 Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

 e-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

Staff and the e-Safety Policy
 All staff will be given the School e-Safety Policy and its importance explained.

 Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

 Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

 Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting Parents' and Carers' Support

 Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

 The school will explain to all parents the importance of e safety and will offer to support to parents who wish to discuss e-Safety

 The school will maintain a list of e-Safety resources for parents/carers