



Lancaster Road Primary School

E-Safety/ICT Pupil Acceptable Use

At Lancaster Road Primary School it is believed that the use of ICTs brings great benefits. Recognising the e-safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications.

ICT is a central part of the curriculum as it plays an ever-increasing role in children's lives. On-line access is recognised as a means to support learning across the curriculum. This policy provides a framework for the safe and appropriate use of the Internet for pupils and staff. This policy should be used in conjunction with other related school documentation and policies and particular reference paid to the Anti Bullying Policy, PSHE Policy and Child Safety. This policy focuses on reducing the potential dangers of using technologies whilst ensuring our children gain the maximum benefit from the technologies available in school. E-safety is taught as an integral part of our curriculum and staff, pupils and parents are updated on an annual basis and more frequently if required.

- 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.
- 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 information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Using the internet in education allows:

- Access to world-wide educational resources including museums and art galleries for both pupils and staff;
- Access to expert up to date knowledge for both pupils and staff;
- Fast communication links to support services, professional associations and colleagues;
- Fast exchange of data with the LEA and DfE/DfCSF.

Internet use will enhance learning because

- Use of the Internet will be built into curriculum planning for all subjects to specifically enrich and extend the learning process;
- Staff will guide pupils in on-line activities that are planned to support the learning outcomes 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.

1. Overview of Issues and Risks

ICT can offer many positive educational and social benefits to pupils, but unfortunately there are some dangers. As in any other area of life, children and young people are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may

find themselves involved in activities which are inappropriate, or possibly illegal. Unmediated Internet access brings with it the possibility of placing pupils in embarrassing, inappropriate and even dangerous situations. Some of the issues and risks are summarised below.

- **Copyright infringement** - Copyright law applies on the internet, but is ignored by many who download and swap music files and copy and paste text and graphics;
- **Exposure to inappropriate materials** - There is a risk that when using the internet, email or chat services, young people may be exposed to material that is pornographic, hateful or violent in nature, encourages activities that are dangerous or illegal, or is just age-inappropriate or biased;
- **Inappropriate or illegal behaviour** - Online bullying is an unfortunate aspect of the use of new technologies, perceived as providing an anonymous method by which bullies can torment their victims at any time, they may receive email, chat or text messages that make them feel embarrassed, upset, depressed or afraid. This can damage their self-esteem and pose a threat to their wellbeing;
- **Physical danger and sexual abuse** - A criminal minority make use of the internet and related services such as chat rooms to make contact with young people. The intention of these people is to establish and develop relationships with young people with the sole purpose of persuading them into sexual activity. There is also a risk that while online a young person might provide information that can personally identify them or others, or arrange to meet people they have met online, so posing a risk to their safety or that of their family or friends;
- **Inappropriate or illegal behaviour by school staff.** - This may include viewing or circulating inappropriate material via email, or much more serious activities such as viewing, possessing, making or distributing indecent images. Inappropriate activity by a staff member may result in a disciplinary response by the school or authorities.

2. Principles of Internet Safety

The School Internet Policy is built on the following five core principles:

Guided Educational Use - Significant educational benefits should result from curriculum Internet use including access to information from around the world and the abilities to communicate widely and to publish easily. Curriculum Internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful Internet use will also reduce the opportunities for activities of dubious worth;

Risk Assessment - Use of the internet poses certain risks as outlined above from which our pupils need to be protected. At the same time they must learn to recognise and avoid these risks - to become "Internet Wise". We will ensure that they are fully aware of the risks, perform risk assessments and implement the policy for Internet use. Pupils need to know how to cope if they come across inappropriate material;

Responsibility - Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies such as mobile phones. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions will be judged carefully;

Regulation - The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access within school must simply be denied, for instance unmoderated chat rooms present immediate dangers and are banned. Fair rules, clarified by discussion and prominently displayed at the point of access will help pupils make responsible decisions;

Appropriate Strategies - This policy describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities. There are no straightforward or totally effective solution and staff, parents and the pupils themselves must remain vigilant;

3. **Creating a Safe ICT Learning Environment**

The first challenge in creating a safe ICT learning environment is to ensure that everyone is aware of the issues and how they impact upon the school environment and the pupils. Awareness will be raised, in part, by a comprehensive internet safety education programme for the whole school community. The programme will be continuous, responding to specific incidents and issues, and providing information about emerging technologies as well as those already embedded within the culture of the school. A person with the designated role of internet safety co-ordinator has been created within the school to develop and monitor e-safety policies.

4. **Roles and Responsibilities**

Internet Safety Co-ordinator

- The primary responsibility of the internet safety co-ordinator will be to establish and maintain a safe ICT learning environment within the school. Working with the other staff such as technician and the headteacher to develop, or review, appropriate internet safety policies and procedures;
- Leading the development of management protocols so that any incidents in which internet safety is breached are responded to in an appropriate and consistent manner, with the appropriate authority to take action as necessary;
- Leading in the creation of a staff professional development programme that addresses both the benefits and risks of communication technologies;
- Leading in the creation of an internet safety education programme for pupils, maintaining an overview of activities across the school, and supporting staff with information and resources as appropriate;

- Developing a parental awareness programme;
- Maintaining a log of all incidents relating to internet safety in school;
- Updating the governing body on current internet safety issues, in conjunction with the headteacher;
- Liaising with outside agencies, which may include the LEA, local schools, or national agencies, as appropriate.

Headteacher

- Taking ultimate responsibility for internet safety issues within the school, while delegating day-to-day responsibility to the internet safety co-ordinator;
- Supporting the internet safety co-ordinator in creating an internet safety culture within the school, including speaking to staff and pupils in support of the programme;
- Ensuring that the governing body is informed of the issues and the policies;
- Ensuring that appropriate funding is allocated to support internet safety activities; throughout the school, for both the technical infrastructure and Inset training promoting internet safety across the curriculum.

Governing Body

- The Governing body has statutory responsibilities for child protection and health and safety, and elements of these will include internet safety;
- At Lancaster Road main responsibilities related to e-safety are delegated to the Curriculum Committee;
- Developing an understanding of existing school policies, systems and procedures for maintaining a safe ICT learning environment and supporting the headteacher and e-safety co-ordinator in implementing these, including ensuring access to relevant training for all school staff;
- Promoting internet safety to parents, and providing updates on internet safety policies within the statutory 'security' section of the annual report.

Classroom Teachers and Teaching Assistants

- Develop and maintain knowledge of internet safety issues, particularly with regard to how they might affect children and young people;
- Implementing school policies through effective classroom practice;
- Ensuring any instances of ICT misuse, whether accidental or deliberate, are dealt with through the proper channels, reporting to the internet safety co-ordinator in line with school internet safety policies;
- Planning classroom use of the internet and ICT facilities to ensure that internet safety is not compromised; for example, evaluating websites in advance of classroom use and ensuring that school filtering levels provide appropriate protection for topics being studied;
- Embedding teaching of internet safety messages within curriculum areas wherever possible;
- Maintaining an appropriate level of professional conduct with their own internet use both within and outside school.

Pupils

- Upholding school policies relating to acceptable use of the internet and other communications technologies;
- Developing their own set of safe and discriminating behaviours to guide them whenever they are online;
- Reporting any incidents of ICT misuse within school to a member of the teaching staff;
- Seeking help or advice from a teacher or trusted adult if they experience problems when online, or if they receive any content or contact which makes them feel uncomfortable in any way;
- Communicating with their parents or carers about internet safety issues, and upholding any rules for safe internet use in the home.

4.2 Technological Tools

- The school will work in partnership with the LEA to ensure systems are in place to protect pupils and that they are reviewed and improved;
- An LEA filtering system is in place to minimise access to inappropriate content via the school network;
- If staff or pupils discover unsuitable sites or images, the URL (address) and content must be reported to the e-safety co-ordinator, who has the ability to block the site from within school. The LA via BTLS will also be informed;
- It will be possible to keep track of web pages visited and downloaded files to help investigate possible issues and monitor internet usage;
- Pop up blockers and virus protection will be installed on every computer in the school to minimise further risk of access to inappropriate materials.

4.3 Internet Safety Education Programme for the Whole School Community

Pupils

It is important that teachers, parents and carers do not confuse skilful use of new technologies with an ability to perceive and avoid risk - internet and ICT literacy is unfortunately not synonymous with internet and ICT safety. Internet safety and related school policies will therefore be carefully introduced to pupils.

- The school will use Internet Proficiency Schemes for pupils to specifically teach internet safety skills;
- While discrete lessons are useful, internet safety concepts should be embedded within the curriculum wherever possible, while safety messages should be reinforced every time pupils use the internet and related technologies;
- Instruction in responsible and safe use should precede Internet access;
- 'Rules of Internet use' will be posted near to computer systems. Pupils will be reminded of their acceptance of the rules and related consequences should the rules be breached;
- Pupils will be informed that internet use will be monitored;

- Pupils should be taught to be critically aware of the materials they read and know that material is not necessarily valid just because it is on the Internet;
- Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

Parents

Parents and carers also have a key role to play in creating a safe ICT learning environment and culture, through promoting internet safety at home and hence reinforcing the messages taught in school.

The children are taught to use the internet sensibly. It is recommended that parents also develop a similar set of rules if their children are using the Internet at home. In this way, we can promote responsible and safe internet use at home and in school:

- Parents' attention will be drawn to the School Internet Policy in newsletters, the school prospectus 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 and useful websites will be made available to parents via the school website.

4.4 E-mail Management

- Pupil access to e-mail in the school is via Lancashire's e-mail management system only. Each class has an e-mail account and all staff have their own Lancashire account;
- A responsible adult will supervise pupils when writing and sending e-mails and the content of outgoing and incoming e-mails should be checked by the adult (ICT co-ordinator or the class teacher);
- Children will be taught to never reveal personal details such as home addresses or telephone numbers during e-mail dialogue;
- Pupils will be taught to write polite and responsible e-mails;
- The ICT co-ordinator and class teachers have responsibility to ensure that no abuse of the e-mail facility occurs;
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

4.5 Newsgroups, Chat Rooms and Instant Messaging

- Pupils will not be allowed access to public or unregulated chat rooms, newsgroups or instant messaging services;
- A risk assessment will be carried out before pupils are allowed to use a new technology in school including the use of regulated educational chat room environments.

4.6 Managing Emerging Internet Use

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed;
- Pupils are not permitted to have mobile phones or other hand held devices in school. If a parent or carer has specifically requested their child brings a device into school, it must be stored in the school office until the end of the day.

5. Web Site Content Management

The school has a school website for the purpose of keeping parents informed about important, dates and events as well as providing information about the school and its related policies. Including images of pupils on the school website is motivating for the pupils and provides a good opportunity to promote the work of the school policies. The school will consider the threat of inappropriate use of images of children:

- 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 pupil names will not be shown;
- Images of pupils in suitable dress only will be used;
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site;
- The Headteacher 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.

6. Safe and Appropriate Management of Digital Images

The school has given consideration to the way in which digital images including video are captured and stored within school for the protection of both pupils and staff. Each year group will be provided with its own digital camera. Staff are made aware of the appropriateness of holding images on personal digital cameras and video. Pupils may also be involved in video conferencing activities. Specifically:

- Images will be taken and stored on school equipment. If images are taken with personal equipment they should be transferred to the school network or web site as soon as possible and deleted from the camera before it is taken off site;
- All images and video should be stored on the school network or school website;
- It is recognised that some images may need to be filed by staff in other areas, such as pupil and subject portfolios. Staff will have given consideration to the amount and appropriateness of the images;
- Written permission from parents and carers will be obtained before children take part in film making and video conferencing projects;
- Images no longer required for pupil portfolios, subject portfolios, school promotion and use on the website will be deleted on an annual basis;
- Images of pupils who have left the school will be deleted.

7. Internet Access Authorisation

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff leaving or the withdrawal of a pupil's access;
- Parents will be informed that pupils will be provided with supervised Internet access;
- Written permission from parents or carers will be obtained before any type of internet access is allowed;
- At Key Stage 1, access to the Internet will be by adult demonstration and directly supervised access to specific, approved sites. Internet access at lower Key Stage 2 will follow the same format, although the range of sites available will increase;
- Pupils in upper Key Stage 2 may, under supervision, use search engines to carry out approved searches. Searches using 'child friendly' search engines such as 'Ask Jeeves for Kids' and 'Yahooligans' is recommended;
- Pupils may not use the internet at breaktimes or lunchtimes, if unsupervised.

8. Staff Consultation

- All staff must accept and sign 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, will be given access to the School Internet Policy, and its importance explained.
- 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.
- Staff development in the safe and responsible Internet use, and on school Internet policy will be provided as required.

9. Responding to Incidents of Misuse

Minor Incidents

- Minor incidents of misuse by pupils might include; copying information into work and failing to acknowledge the source - plagiarism, downloading materials or images not relevant to their studies, and misconduct associated with pupils files, such as using someone else's password or deleting someone else's files.
- In all cases the pupils will be issued with a warning and referred back to the rules of internet use. The incident should be documented.
- The internet safety co-ordinator will monitor minor incidents to identify trends in pupils' behaviour, and will react to any emerging issues. This might include raising awareness on a particular internet safety topic at a school assembly or offering staff additional training.

Incidents Involving Inappropriate Materials or Activities

- Specific breaches of policy and rules might include deliberately accessing, printing, showing or transmitting inappropriate (or age-restricted) material within the school's network.
- Serious incidents relating to internet safety in schools will be reported to the internet safety co-ordinator immediately. The internet safety co-ordinator must

document the incident and decide on an appropriate course of action, which may include involving the headteacher and external agencies. It may also be necessary to involve child protection

- Staff to provide follow-up counselling and support .
- The internet safety co-ordinator will review internet safety policies as soon as possible after the incident in an attempt to prevent such an incident recurring, debriefing relevant staff accordingly, and providing school-wide training as appropriate.
- If a child discovers something on the internet that makes them feel uncomfortable or upset, they must report it immediately to their teacher. Pupils will be taught to turn off the monitor or close the lid of the laptop so that attention is not drawn to the material.
- Although Internet access at Lancaster Road Primary is filtered, there may be occasions when inappropriate material gets through. The site must be reported immediately to the Internet Safety Co-ordinator who will ensure that the website is added to Lancashire's list of blocked sites and is filtered from within school.

Incidents involving illegal materials or activities

- Discovery of indecent material within the school's network is a very serious situation, and must always be reported to the police. It is important that the material is not downloaded, printed or sent by email, because doing so will be an offence in itself. If at all possible, do absolutely nothing to the suspect computer or computers, including turning them on or off. It may be necessary to shut down the whole network, but do not do this unless instructed by the police. Ensure that everyone is kept away and that nothing is touched. Under no circumstances should the internet safety co-ordinator, network manager or headteacher attempt to conduct an investigation of their own, or bring in an outside 'expert' to do so, as this may compromise the evidence if a legal case were to result. In some cases this may constitute a criminal offence in itself.

10. Sanctions

- If a pupil misuses e-mail or the internet, they must be reminded that this is irresponsible and contrary to their agreement with the Internet Acceptable Use Policy. They must agree to responsibly use the internet and a further copy of the Acceptable Use Policy will be sent home for the child and parent to sign. A record of misuse will be logged by the Internet security co-ordinator. The child will not be allowed to resume the use of the internet until the AUP has been resigned by the parent and child. Minor transgressions can be dealt with by the teacher as part of normal school discipline policy
- In serious circumstances the privileges of internet use will be withdrawn for a fixed period of time

11. Monitoring

- The Internet Safety co-ordinator will monitor any logged incidents and assess their importance.
- Pupils will be informed their internet use can be monitored. Monitoring checks will be made if any inappropriate use is suspected.

- The Internet safety co-ordinator will report on incidents and the effectiveness of the e-safety policy to the governing body on an annual basis.

12. Review

Due to the nature of the internet and emerging technologies this policy will be reviewed on an annual basis.

References and Resources

http://www.lancsngfl.ac.uk/esafety/index.php?category_id=3

http://www.kenttrustweb.org.uk/kentict/kentict_esafety_home.cfm