Lower Darwen Primary School

We are proud of our school.

E-Safety Policy

Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Tablets
- Other mobile devices with web functionality

At Lower Darwen Primary School we understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. This policy is inclusive of both fixed and mobile internet; technologies provided by the school; (such as I.pads, PCs, laptops, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones and portable media players, etc).

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the e-Safety coordinator along with the Leadership Team to keep abreast of current issues and guidance through organisations such as BwD LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Writing and reviewing the e-Safety policy

This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies including those for computing, Behaviour for Learning, Health and Safety, Child Protection (Safeguarding), Prevention of Radicalisation and Extremism and PSHE policies including Anti-bullying.

E-Safety skills development for staff

- Staff receive regular information and training on e-Safety issues through the coordinator at staff meetings.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff receive information on the school's Acceptable Use Agreement as part of their induction.
- All staff are encouraged to incorporate e-Safety activities and awareness within their lessons.

E-Safety information for parents/carers

1. Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
2. Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website.
3. The school will send out relevant e-Safety information through newsletters, the school website, text messages and via dojo messaging.

Community use of the Internet

External organisations using the school's computing facilities must adhere to the e-Safety policy.

Teaching and Learning

Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teach e-Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff.
- 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 encouraged to use the 'Hector Protector' button to hide any material that they know is unsuitable for viewing. This will instantly cover the whole screen until it can be dealt with by the class teacher.
- 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 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 should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.
- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- The school has firewalls and this are checked regularly by Western Business Ltd who maintain our IT systems

Published content and the school web site

The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will **not** be published. The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website. This consent form is considered valid for each year that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully. Pupils' full names will not be used anywhere on the School Website when associated with photographs. Only pictures of groups or group activities will be permitted.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

Photographs taken by parents/carers for personal use

In the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites, e.g. School performances and assemblies etc.

Social networking and personal publishing

- The school will block / filter access to social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location. Our pupils are asked to report any incidents of bullying to the school.
- School staff are advised not to add children as 'friends' if they use these sites.

Managing filtering

- The school will work with the local authority, DCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If pupils or staff discovers an unsuitable site, it must be reported to the class teacher, computing subject leader or head teacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Senior staff will also monitor electronic devices to ensure pupils are not accessing inappropriate sites that promote sexual activity and or radicalisation and extremism.

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.

- The use of portable media such as memory sticks will be monitored closely as potential sources of computer virus and inappropriate material.
- If pupils bring phones to school they must take them to the school office and they will be kept there until the end of the day.
- The sending of abusive or inappropriate text messages outside school is forbidden and the school's behaviour for learning policy extends outside of school hours.
- Staff will use a school phone where contact with parents is required.
- Staff should not use personal mobile phones during designated teaching sessions and in view of pupils.

The school operates SMART rules to protect children on line. These are incorporated into the school's behaviour for learning policy.

Computing/ICT- Smart Rules

The school uses SMART rules when using computers and other devices that access the Internet:

Stay Safe – Don't give out personal information to people/places you don't know
Don't Meet Up- Meeting someone you have only been in touch with online can be dangerous. Always check with an adult you trust
Accepting Files- Accepting e.mails, files, pictures or texts from people you don't know can cause problems
Reliable- Check information before you believe it Is the person or website telling the truth?
Tell Someone- Tell an adult if someone or something makes you feel worried or uncomfortable

On-line safety

Mobile phones, computers and other digital devices can be a source of fun, entertainment, communication and education. However, we know that some adults and young people will use these technologies to harm children. The harm may include sending hurtful or abusive texts and emails; enticing children to engage in sexually harmful conversations online; inappropriate/indecent webcam filming and photography or face-to-face meetings. So called 'sexting' falls into this category.

Children and young people may unknowingly also engage in activities that could put themselves and others at risk, such as revealing personal information and uploading images of others.

Online bullying by pupils, via texts and emails, will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures.

- School policies/measures will encourage good behaviour and respect (this includes around bullying)
- We have an anti-bullying / behaviour for learning policy that links to online safety
- We ensure policies take into account equality and diversity
- We ensure policies relating to searching a student or their property with and without their consent are written correctly
- We have an up to date home / school agreement regarding the use of social media to make complaints relating to pupils

Where a child protection/ safeguarding issues has been raised regarding the use of technologies, this should be reported to the Designated Senior Person and headteacher as with any other Safeguarding concerns. (*see school's Safeguarding policy*)

Prevention of Extremism and Terrorism

Prevent is the government's strategy for preventing extremism and terrorism. Pupils accessing extremist material online, including through social networking sites will be treated as a serious safeguarding issue. These concerns will be reported to the Designated Senior Person and

headteacher and the appropriate action taken. These may include a referral to Channel (see the school's Prevention of Extremism and Radicalisation Policy).

Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism, there is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. From July 2015 all schools are subject to a duty under section 26 of the Counter-Terrorism and Security Act of 2015, to have 'due regard to the need to prevent people from being drawn into terrorism', known as the 'Prevent Duty'.

Protecting personal data

The school will collect personal information about you fairly and will let you know how the school and the LA will use it. The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school or the LA. For other members of the community the school will tell you in advance if it is necessary to pass the information on to anyone else other than the school and the LA.

The school will hold personal information on its systems for as long as you remain a member of the school community and remove it in the event of your leaving or until it is no longer required for the legitimate function of the school. We will ensure that all personal information supplied is held securely, in accordance with the policies and practices of BwD and as defined by the Data Protection Act 1998 and the GDPR regulations (2018).

Stakeholders have the right to view the personal information that the school holds about you and to have any inaccuracies corrected.

Policy Decisions

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Acceptable Use Agreement for pupils and abide by the school's e-Safety rules. These e-Safety rules will also be displayed clearly in all networked rooms.
- Access to the Internet will be by directly supervised access to specific, approved on-line materials.
- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's e-Safety rules and within the constraints detailed in the school's e-Safety policy.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Password Security

Adult users are provided with an individual network, email and Learning Platform login username and password, which they are encouraged to change periodically. All pupils are provided with an individual class login, and Learning Platform login username and password.

- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff know their individual responsibilities to protect the security and confidentiality of the school network.

Assessing risks

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 hardware. The school will audit ICT provision to establish if the e-Safety policy is adequate and that its implementation is effective (including firewalls and filter systems).

Handling e-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff and reported to the e-Safety coordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety coordinator and recorded in the e-Safety incident logbook.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection/safeguarding nature including radicalisation must be dealt with in accordance with school child protection/safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure.

Communications Policy

Introducing the e-Safety policy to pupils

- E-Safety rules will be displayed in all classrooms and the ICT suite and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PSHE lessons/circle times/anti-bullying week.
- Pupils will be informed that network and Internet use will be monitored**.**
- The 'Hector the Protector' e-safety button will be discussed and its use encouraged when inappropriate material is displayed.

Staff and the e-Safety policy

- All staff will be given the School e-Safety policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school
- All children will be given a username and password to access secure resources and facilities on the server.
- The school's web history will be regularly monitored for incidents of cyber-bullying, inappropriate use of language uploading of inappropriate files or searching inappropriate material. Children will be informed that the sending of messages through the school's I.pads computers and laptops is monitored and misuse of the messaging system will result firstly in a warning, followed by removal as a user should such behaviour be repeated.
- Class teachers will monitor the use of the software and hardware. Any misuse of the will be reported to the head teacher who will take appropriate action.

Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the e-Safety Coordinator. This policy is the Governors' responsibility and they will review its effectiveness annually. They will do this during reviews conducted between the e-Safety Coordinator, computing subject leader, and head teacher. Designated Senior person, and Governor with responsibility for ICT and Governor with responsibility for Child Protection will also be involved in the review. Ongoing or serious incidents will be reported to the full governing body.

To be read in conjunction with:

Behaviour for Learning, Internet Security, Safeguarding, Prevention of Radicalisation and Extremism, Remote Learning and Social media policies

This revised document was approved by the Governing Body of Lower Darwen Primary School.

On 16th September 2024
As part of the Behaviour for Learning Policy, Safeguarding Policy
Next review: June 2025