# E-SAFETY POLICY

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children should have an entitlement to safe internet access at all times.

The requirement to ensure that children are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Email and Instant Messaging
- Blogs
- Video Broadcasting
- Gaming
- Zoom
- Live Streaming
- Learning Platforms & Virtual Environments
- Chat Rooms and Social Networking
- Podcasting
- Music Downloading
- Mobile / Smart Watches/ Smart Phones with text, video and / or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed.  All users need to be aware of the range of risks associated with the use of these Internet technologies. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication with others, including strangers.
- Cyber-bullying.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the child's social and emotional development and learning.
- Inappropriate content or exposure whilst using live streaming platforms.

At Leighton Academy we understand the responsibility to educate our pupils on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Policy (for all staff, local advisory board members , visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, netbooks, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by staff, but brought onto school premises (such as laptops, mobile phones and camera phones).

**Schedule for Monitoring & Review**

| | |
|---|---|
| The implementation of this e-safety policy will be monitored by the: | E Safety Lead – Samantha Thompson supported by Sophie Abrams and Zoe Dow |
| Monitoring will take place at regular intervals: | Annually |
| The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: | Next Review Date:<br>January 2022 |
| Should serious e-safety incidents take place, the following external persons should be informed: | Depending on the seriousness of the incident: CEOP trained, Sophie Abrams and Zoe Dow should be informed and there is the CEOP report button on the Think U Know website. The principal should also be informed and the police will be involved where appropriate. |

**Scope of the Policy**

This policy applies to all members of the academy community who have access to and are users of ICT systems, both in and out of the building.

The Education and Inspections Act 2006 empowers principals, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy site. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of the academy. The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will inform parents / carers of incidents of inappropriate e-safety behaviour.

Any inappropriate language regarding Lesbian, Gay, Bisexual, Transgender, Queer or other (LGBTQ+) and online bullying both on school computers and outside of school will not be tolerated and that the same sanctions apply to online LGBTQ+ bullying as in the classroom.

This policy, supported by the academy's acceptable use agreements for staff, local advisory board, visitors and pupils, is to protect the interests and safety of the whole community. It is linked to the following mandatory policies: child protection and safeguarding, acceptable use, cameras and mobile phones, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy, CCTV and Personal Development.

**Roles and Responsibilities**

As E-Safety is an important aspect of strategic leadership within the academy, the principal and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-Safety Lead in our school is Samantha Thompson supported by Sophie Abrams and Zoe Dow.

**Local Advisory Board (LAB)**

LAB Members are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. Senior management and LAB members are updated by the principal / E-Safety Lead.

**Principal and Senior Leaders**

- The principal is responsible for ensuring the safety (including e-safety) of members of the academy community.
- The principal is responsible for ensuring that staff receive suitable CPD to enable them to carry out their e-safety roles.
- The principal will ensure that there is a system in place to allow for monitoring and support of those in the academy who carry out the internal e-safety monitoring role.
- The principal is aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

**E-Safety Lead**

Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

- Provides training and advice for staff.
- Liaises with other agencies
- Liaises with the Computing Lead.
- Receives reports of e-safety incidents.
- Attends relevant LAB meetings.
- Keeps abreast of current issues and guidance through organisations such as Education Bradford, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

**The Computing Lead**

The Computing Leadr is responsible for ensuring:

- That the academy's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the academy meets the e-safety technical requirements.
- That users may only access the academy's networks through a properly enforced password protection policy.
- That the academy uses Exa Networks filtering service.
- That any misuse / attempted misuse of the network / Virtual Learning Environment (VLE) / email is reported to the E-Safety Lead.

**Staff**

- New staff receive information on the academy’s acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know to report the misuse of technology by any member of the academy community to the E-Safety Lead.
- All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas.

Teaching and support staff are responsible for ensuring that:

- Digital communications with pupils should be on a professional level.
- They monitor ICT activity in lessons and extra-curricular activities.
- They are aware of e-safety issues related to the use of all electronic devices.

**Designated Person for Child Protection and Safeguarding**

The designated person for child protection and safeguarding is trained in e-safety issues and is aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

**Pupils**

- Are responsible for using the ICT systems in accordance with the Acceptable Use Policy, which they (or their parents / carers) will be expected to sign before being given access to systems.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

**Parents / Carers**

Parents and carers will be responsible for:

- Endorsing (by signature) the Acceptable Use Policy
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on the academy website)
- Parent/Carers are responsible for ensuring their children are appropriate, well behaved and follow the home school agreement, whilst on any online Zoom sessions.
- Children and their Parents/Carers have received a home school agreement regarding their Zoom sessions, which highlights that they must not share any meeting links or take photographs of their online sessions.

**Managing the E-Safety Messages**

- We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used.

- E-Safety rules are displayed in every classroom.
- Pupils will be informed that Internet use will be monitored in acceptable use policy.
- All staff will be given the E-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic is monitored and traced to the individual user on any school device at school and off the premises. Discretion and professional conduct is essential.
- Parents' attention will be drawn to the E-Safety Policy in weekly updates and on the website.

**Continuing Professional Development**

Training will be offered as follows:

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the e-safety policy and acceptable use policies.
- The E-Safety Lead will receive regular updates through training sessions and by reviewing guidance documents.
- This E-Safety policy and its updates will be presented to staff.

**Training – LAB Members**

LAB Members should take part in e-safety training / awareness sessions. This may be offered by:

- participation in training / information sessions.

**Equipment, filtering and monitoring**

**Filtering**
The academy will work in partnership with other agencies to ensure filtering systems are as effective as possible.

**Managing Emerging Technologies**
Emerging technologies will be examined by the computing lead for educational benefit and a risk assessment will be carried out before use in the academy is allowed.

**Information System Security**

- ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Learning for Life Partnership and Exa Networks.

**Equipment**

- Servers, wireless systems and cabling must be securely located and physical access restricted
- The "administrator" passwords for the ICT system, used by the Learning for Life Partnership and the Computing Lead.
- Executable files can only be run using the "administrator" rights.
- See iPad and laptop policy for information about devices which are taken off the premises.
- The network and individual workstations are protected by up to date virus software.

**Monitoring**

- There will be regular reviews and audits of the safety and security of ICT systems
- Surf protect, which is accessed through Exa Networks, is used to regularly monitor and record the activity of users on the school ICT systems.

**Curriculum**

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety. Please see curriculum overview

E-Safety education will be provided in the following ways:

- The academy follows the curriculum 2014 requirements and Purple Mash platform to teach children about E-Safety.
- Educating all pupils on the dangers of technologies that maybe encountered outside school is done formally as part of the computing curriculum.
- Pupils are 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 staff member, or an organisation such as ChildLine/ CEOP report abuse button.
- E-safety messages are reinforced in assemblies.
- Pupils are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside the academy.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination).
- The E-Safety team work closely with the PCSO's to deliver E-safety lessons.

**Equal Opportunities**

The academy endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of our E-Safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well managed for these children and young people.

**Managing the Internet**
**Use of the Internet to Enhance Learning**

- The academy internet access is designed for pupil use and includes filtering.
- Pupils are taught what internet use is acceptable and what is not.
- Internet access will be planned to enrich and extend learning activities.
- Staff will preview any recommended sites before use.

- Staff will guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge, location, retrieval and evaluation.

**Authorised Internet Access**

- All staff must read and sign the 'Acceptable Use Policy' before using any academy ICT resource.

**Internet**

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the support technician via the principal.
- The academy will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- It is the responsibility of the academy, by delegation to the network manager to ensure that anti-virus protection is installed and kept up to date on all academy machines.

**Email**

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of Leighton Academy, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, either staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'.

- The academy gives all staff their own email account to use for all academy business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all academy business.
- Under no circumstances should staff contact pupils, parents or conduct any academy business using personal email addresses or phone numbers. During the lockdown period, staff have been using 'no caller ID' to make calls to families from their personal phones.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in the academy to external personal e-mail accounts may be blocked.

**Social Networking**

The use of public social networking sites (e.g. Twitter, WhatsApp, Snapchat, Instagram, TikTok, YouTube and Facebook) is not allowed in the academy with the exception of the principal's access to the school Facebook and Twitter accounts.

The academy will block/filter access to social networking sites and newsgroups unless a specific use is approved.

- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils are taught not to place personal photos on any social network space.
- Both, the class teachers and the PCSO's deliver lessons around social networking. This is to ensure, children understand the dangers of these platforms and how to keep themselves safe online.

**Data Protection**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

The key principles can be found in the Academy's **Data Protection Policy**.

Staff must ensure that they:

- At all times, take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- Where staff are working from home, they must ensure they follow the home learning risk assessment, which highlights how to act appropriately whilst providing remote learning.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device once it has been transferred or its use is complete.

**Assessing Risks**

- The academy will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on an academy computer.
- The academy will audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate.
- Currently pupils are not allowed to use personal mobile devices/phones in school. KS2 children, who may be walking home alone, carry a mobile phone but must give this to their class teacher as soon as they enter the classroom. This is at parents' own risk.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.

**Responding to incidents of misuse**

If any apparent or actual misuse appears to involve illegal activity contact the safeguarding lead immediately i.e.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct,  activity or materials

Pupils are encouraged to inform their teacher or other adults in the academy regarding anything which makes them feel uncomfortable while using ICT.

- Complaints of Internet misuse will be dealt with by the principal and recorded on CPOMS
- Any complaint about staff misuse must be referred to the principal.
- Complaints of a child protection nature must be reported to the Named Persons for Child Protection.

**(See also Safeguarding and Whistle Blowing Policies)**