ONLINE SAFETY POLICY FOR LEIGHTON ACADEMY

Policy lead:	Mrs S Hargreaves
Approval date:	01.09.25
Next review date:	01.09.28
Approval needed by:	LGB

Leighton Academy is part of The Learning Partnership.

Leighton Academy's Online Safety Policy

At Leighton Academy, we believe that the use of online services and tools can provide enhanced collaborative learning opportunities, high engagement, allow access to rich and up-to-date content and can support the needs of all our pupils. We embed the use of online technologies throughout the school as part of learning and we also aim to give pupils the skills to interact with the ever-changing online world in a balanced, healthy and safe way. This is achieved through both implicit measures such as automatic filtering of content and explicit measures including teaching of online safety. Additionally, clear rules are established for the use of devices and the internet by any people in school; we ensure that online safety is maintained and pupils' needs are met. We aim to equip pupils with the skills, strategies and knowledge that will help them gain the benefits of the online world, whilst being able to minimise risk to themselves or others.

Pupils must be prepared for the connected world ahead of them, including:

- Websites and online search engines
- Email and instant messaging, such as WhatsApp
- Blogs
- Video streaming - pre-recorded content, which is often found on sites such as YouTube
- Live streaming, which is increasingly popular on gaming platforms
- Multiplayer gaming, both with 'real world' friends, online friends and strangers
- Virtual reality
- Artificial intelligence
- Mobile devices, smart watches, smart phones with text, video and web functionality
- Learning platforms and virtual environments such as Purple Mash
- Social Networking and video chats, including the chat functions within online games
- Music streaming and podcasting

Whilst exciting and beneficial, both in and out of the context of education, much IT, 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.

As part of the digital literacy section of our programme of study, online safety is not only taught discretely through these computing sessions, but additionally during Personal Development and Citizenship lessons, whole school opportunities for learning such as assemblies or event days, as well as during other subjects where pupils might use technology.

This policy has been developed in collaboration with Sam Thompson (Online Safety Lead), Philly Lockitt (DSL) and Sophie Hargreaves (Computing Lead) and will be monitored annually or more regularly in the light of any significant developments in the use of technologies, new threats to online safety or incidents that have taken place.

This policy should be read in conjunction with:

- Computing Policy
- CCTV Policy
- Child Protection and Safeguarding Policy
- Personal Development Policy
- RSH and Health Education Policy
- Social Media Policy
- Complaints Policy
- Data Protection (GDPR) Policy
- Acceptable Use Agreements – for staff and pupils
- Anti-Bullying (KiVa) Policy
- Staff Code of Conduct
- Behaviour Regulation Policy
- Disciplinary Policy
- Remote Learning Policy
- Whistleblowing Policy

The legislative guidance that has helped formulate key parts of the policy are listed below. The policy conforms to the latest government initiatives and revisions to existing legislative guidance which are applicable to Online Safety:

- UK Council for Child Internet Safety (2020)
- UK Council for Child Internet Safety (2017)
- Sexting in schools and colleges: Responding to incidents and safeguarding young people
- DfE Keeping Children Safe in Education (2024)
- DfE Teaching Online Safety in Schools (2019)
- DfE Searching, screening and confiscation (2018)
- Voyeurism (Offences) Act 2019
- The General Data Protection Regulation (GDPR)
- The Data Protection Act (2018)
- Education for a Connected World

Aims of the Policy

At Leighton Academy, we understand the responsibility to educate our pupils on online safety issues. We teach them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies.

Considering the online safety of our pupils, we have used the following categories of risk:

- **Content** - being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.

- **Contact** - being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.

- **Conduct** - personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and financial scams.

This policy aims to anticipate these risks and safeguard against them:

- To ensure that automatic protections such as filtering are in place and kept up to date with evolving risks.
- To teach a relevant, up-to-date online safety curriculum, which is progressive from Early Years to the end of Year 6.
- To thread the teaching and reinforcement of online safety understanding through all subjects and embed it in the day-to-day lives of pupils and staff.
- To train staff and governors in the latest methods of enhancing the online safety of all pupils and respond to new threats to pupils' online safety.
- To communicate with pupils about their experiences, understanding and concerns through pupil voice surveys and as part of learning walks.
- To advise parents regarding protecting online content in the home and on devices used by pupils.
- To have in place, up to date acceptable use contracts for pupils, parents and staff.
- To provide clear guidance in the correct monitoring and reporting of online safety incidents.
- To have clear guidance about the steps to take in the case of incidents related to online safety.
- To have data policies outlining how we keep data secure.

Scope of the Policy

This policy applies to all members of the academy community who have access to and are users of IT 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 online 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 online 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.

Curriculum

Online safety is embedded throughout the curriculum however it is particularly addressed in the following subjects:
• Computing
• RSE (Relationships and Sex Education)
• Personal Development and Citizenship

The curriculum and the school's approach to online safety is developed in line with the DfE's 'Teaching online safety in school' guidance and the associated UK Council for Child and Internet safety's 'Education for a connected world framework.' In the Autumn term each year, we use the Online Safety units from the Purple Mash Computing Scheme of Work to teach many aspects of online safety within the context of Computing as a subject. This aims to give pupils the underpinning knowledge of aspects of the online world to help them develop behaviours that can navigate safely and confidently regardless of the device platform or app they're using. It also aims to help pupils develop appropriate scepticism and reasoning when they encounter new online experiences to be able to evaluate the risks or potential pitfalls of these encounters. We further reinforce and expand this teaching through the Personal Development and RSE curricula, which also covers aspects of online safety. We supplement this teaching with whole school online safety awareness through assemblies, specialist visiting speakers such as PCSOs and through role modelling in the day-to-day life of the school. Online safety teaching is appropriate to pupils' ages and developmental stages as well as being flexible enough to be tailored to any specific emerging threat within the community.

The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- Evaluating what they see online
- Recognising techniques used for persuasion
- Clear understanding of acceptable an unacceptable online behaviour
- Identifying online risks
- How to seek support

Further to the online safety modules on the Purple Mash Scheme of Work, we teach additional online safety lessons through The National Online Safety Scheme in the Spring and Summer term. These lessons are based on some of the topics outlined in the UKCIS Education for a Connected World Framework:

- Self-image & identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information

In Year 5 and 6, teachers follow the gender neutral, age appropriate video resource called 'Alright Charlie' in the Summer term, which helps raise awareness of child sexual exploitation (CSE) in primary schools.

External resources are reviewed by teachers prior to using them for the online safety curriculum to ensure that they are appropriate and to ensure that they are valid sources of information based upon evidence and of high quality. When external visitors are invited into school to deliver certain aspects of the online safety curriculum, the principal and DSL ensure that the visitors selected are appropriate. Before conducting a lesson or activity on online safety, the class teacher and DSL

consider the topic that is being covered and the possibility that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises staff members on how best to support any people who may be especially impacted by lesson or activity. Lessons and activities are planned so they do not draw attention to individual pupils who may be experiencing difficult circumstances. If a staff member is concerned about anything pupils raise, they will make a report in line with the safeguarding and child protection policy.

Resources

The technology resources used in school to access the internet include:

- Desktop computers
- Laptops
- Tablets
- Interactive whiteboards

The following functions are in place to protect content:

- Content filtering
- Security features such as anti-virus software and firewalls
- Protection against unauthorized installation of software; admin management

All websites used are evaluated by the teacher prior to classroom use.
Staff adhere to copyright laws when creating materials for use in school.
Access is only given to staff and pupils once acceptable use agreements have been signed.
Children use the internet under supervision and with direction in school.

The principal and IT technician ensures that filtering is in place. This is provided by NetSweeper. Filtering is selected to be suitable for the pupils' ages, number of users on the network, not over-blocking or too restrictive. The IT technician regularly reviews the safety and security of IT systems. Any inappropriate usage must be reported to the IT technician to investigate immediately. Any changes to the filtering must be authorised by the principal in consultation with the IT technician and the DSL.

If anyone, including pupils, deliberately breach the filtering in place, this matter is managed through the behaviour policy (pupils) or the disciplinary policy (staff).
If any illegal material is believed to have been accessed this matter will be passed immediately to the appropriate agency e.g. CEOP or the police.

The DSL manages any situations relating to improper use or function of the filtering systems.

All network users have their own usernames and passwords. Users are responsible for keeping their passwords private.
Staff must change passwords every six months.
Users must lock devices when unattended.

Assessment

For Computing, pupil attainment is assessed using the 2Simple Computing Assessment Tool for Years 1 to 6. The tool enables staff to accurately identify attainment of pupils through the detailed exemplification.
Teachers keep accurate records of pupil attainment by entering data using the 2Simple Computing Assessment Tool.

Tracking of attainment by using the 2Simple Computing Assessment Tool is used to inform future planning. Through using the progression of skills documents and displays from 2Simple, both teachers and pupils can evaluate progress.
Work from a range of classes and abilities can be shared using the Noticeboard feature in Purple Mash.
In addition to the Computing Assessment Tool, the pupils complete a concept map at the start of a unit and revisit this at the end of the unit.

Inclusion

We aim to enable all pupils to have a thorough understanding of how to protect their own and others' safety online. This includes children of all abilities, social and cultural backgrounds, those with SEND and EAL speakers. We place particular emphasis on the flexibility technology brings to allowing pupils to access learning opportunities, particularly pupils with SEN and disabilities. With this in mind, we will ensure additional access to technology is provided throughout the school day and in some cases beyond the school day.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less a comprehensive support network from family and friends in staying safe online e.g. pupils with SEND and LAC. Relevant members of staff e.g. the SENCO and designated teacher for LAC work together to ensure the curriculum is tailored so these pupils receive the support they need.

Monitoring

Monitoring will be achieved through:

- Observations
- Pupil and teacher voice
- Learning walks
- Work scrutiny
- Reflective teacher feedback
- Learning environment monitoring
- Dedicated leadership time

Evaluation and Feedback will be achieved through:

- Dedicated leadership time
- Using recognised national standards for benchmarking
- Feedback on whole school areas of development regarding online safety given and discussed during staff training and staff meetings

Concerns regarding a staff member's online behaviour are to be reported to the principal in line with the Staff code of Conduct and Disciplinary Policy.
Concerns regarding a pupil's online behaviour are to be reported to the DSL who will investigate in line with the Child protection and safeguarding and Behaviour policies with the principal and with the support of the IT technician, if required.

The DSL records all online safety incidents on CPOMs.

Staff

- All staff receive safeguarding and child protection training which includes online safety training during their induction.

- All staff receive regular online safety updates at least annually.

- The DSL and deputies undergo training and receive regular online safety updates.

- All staff are informed about how to report online safety concerns in accordance with the relevant policies.

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the online safety policy and acceptable use policies.

- The Online Safety Lead will receive regular updates through training sessions and will review guidance documents, which will then be shared with staff.

- All staff have access to online CPD through Purple Mash and The National Online Safety platform.

- LGB Members should take part in online safety training/awareness sessions

The Wider Community

The school works in partnership with parents to help ensure pupils have a support network to keep them safe online and to reach out to for help. Parents are sent a copy of the Acceptable Use Agreement at the start of each academic year to read with their child.

The school provides information for parents and carers through:

- regular parents' evenings
- signposting to parent online safety material
- website updates
- newsletters

Roles and Responsibilities

As online 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 Online Safety Lead in our school is Samantha Thompson supported by Sophie Hargreaves.

Local Governing Board (LGB)
LGB Members are responsible for:

- The approval of the Online Safety Policy
- Reviewing the effectiveness of the policy.

Principal and Senior Leaders
The Principal and Senior Leaders are responsible for:

- Providing updates to LGB members

- Ensuring the safety (including online safety) of members of the academy community
- Ensuring that staff receive suitable CPD to enable them to carry out their online safety roles
- Ensuring that there is a system in place to allow for monitoring and support of those in the academy who carry out the internal online safety monitoring role
- Being aware of the procedures to follow in the event of a serious online safety allegation being made against a member of staff

Online Safety Lead
The Online Safety Lead is responsible for:

- Ensuring all staff are aware of the procedures that need to be followed in the event of an online safety incident
- Providing training and offering advice for staff
- Liaising with agencies
- Liaising with the Computing Lead
- Receiving reports of online safety incidents
- Attending relevant LGB meetings
- Keeping informed of current issues and guidance through organisations such as Education Bradford, Becta, CEOP (Child Exploitation and Online Protection) and Childnet

Computing Lead
The Computing Lead is responsible for:

- Ensuring the academy's IT infrastructure is secure and is not open to misuse or malicious attack
- Ensuring the academy meets the online safety technical requirements
- Ensuring users may only access the academy's networks through a properly enforced password protection policy
- Ensuring the academy uses NetSweeper filtering service
- Ensuring any misuse/attempted misuse of the network/Virtual Learning Environment (VLE)/email is reported to the Online Safety Lead and IT technician
- Ensuring the online safety curriculum is being delivered to all pupils
- Evaluating emerging technologies for educational benefit and risk assessing prior to use in the academy

Staff
The staff are responsible for:

- Reading and understand the academy's acceptable use policy as part of their induction
- Understanding their individual responsibilities relating to the safeguarding of children within the context of online safety and know to report the misuse of technology by any member of the academy community to the Online Safety Lead
- Delivering online safety activities and creating awareness within their curriculum areas
- Remaining vigilant in monitoring the content of the websites pupils visit

Teaching and support staff
Teaching and support staff are responsible for:

- Ensuring that digital communications with pupils remain on a professional level
- Ensuring computing activities in lessons and extra-curricular activities are monitored
- Ensuring that they are aware of online 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 responsible for:

- Ensuring they have the appropriate training in online safety issues
- Ensuring they are aware of the potential for serious child protection issues to arise from sharing of personal data, access to illegal/inappropriate materials, inappropriate online contact with adults/strangers, potential or actual incidents of grooming and cyber-bullying

Pupils
Pupils are responsible for:

- Using the IT 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
- understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

Parents/Carers
Parents and carers are responsible for:

- Endorsing (by signature) the Acceptable Use Policy
- Deciding whether they consent to images of their child being taken/used in the public domain (e.g., on the academy website)
- 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.

IT technician
The IT technician is responsible for:

- Working alongside the Computing Lead for support with IT infrastructure
- Evaluating emerging technologies for educational benefit and risk assessing prior to use in the academy
- Reviewing IT systems capacity and security
- Installing and updating virus protection regularly
- Discussing security strategies with The Learning Partnership

<u>Managing the Internet and Online Communications</u>

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 online 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

Authorised Internet Access

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

Staff use of Email and Basecamp as platforms for communication

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 'etiquette'.

- The academy gives all staff their own email and basecamp account to use for all academy business. This is to minimise the risk of receiving unsolicited or malicious emails/ messages 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 and messages are 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.

- Pupils must immediately tell a teacher if they receive an offensive email

- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission

- Access in the academy to external personal email 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 SLT's access to the school's 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

Assessing Risks

- The academy will audit IT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate

- Currently pupils are not allowed to bring 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 IT equipment.

- 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.

Schedule for Monitoring & Review

The implementation of this online safety policy will be monitored by:	Online Safety Lead – Samantha Thompson supported by Sophie Hargreaves and Philly Lockitt
Monitoring will take place at regular intervals:	Annually
The Online 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 online safety or incidents that have taken place. The next anticipated review date will be:	September 2026
Should serious online safety incidents take place, the following external persons should be informed:	Depending on the seriousness of the incident: CEOP trained, Sophie Hargreaves and Philly Lockitt 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.