Online Safety Policy

The use of the Internet as a means to develop learning, understanding and communication has become an integral part of life.

Clearly there are risks involved when using any form of on-line communication which lies within the public domain, therefore it is imperative that there are clear rules, procedures and guidelines to minimise any risks when children and staff use these technologies at LSA.

At LSA we strive to educate our pupils through the Personal Development Curriculum, the ICT Curriculum and in Personal Development/ Internet Safety events. We also aim to support parents in trying to navigate the online world that our children inhabit, with Online Safety Newsletters and other regular correspondence.

While we endeavour to safeguard against all risks, we may never be able to completely eliminate them. Any incidents that may arise will be dealt with quickly and according to our policy to ensure students continue to be protected.

Aims

At LSA we aim to:

- Have robust processes in place to ensure the online safety of all members of our learning community including students and staff
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in our use of technology, including mobile and smart technology
- Establish clear mechanisms and responsibilities to identify, intervene and escalate an incident of concern relating to internet safety

Our approach to online safety considers the following:

1. **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
2. **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention of grooming or exploiting them for sexual, criminal, financial or other purposes
3. **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying. Issues that can arise for young people in the future from bad decisions online.
4. **Commercial Risks** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Our young people need to be able to evaluate what they read and watch, recognise techniques of persuasion, identify online risks and know where to go to for help.

Legislation and guidance

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

Keeping Children Safe in Education 2022, and its advice for schools on *Teaching online safety in schools* 2023, *Preventing and tackling bullying and cyber-bullying: advice for Headmasters and school staff*

It also considers the DfE's guidance on protecting children from radicalisation

· Voyeurism (Offences) Act 2019

· The UK General Data Protection Regulation (UK GDPR)

· Data Protection Act 2018

· DfE (2021) 'Harmful online challenges and online hoaxes'

· DfE (2022) 'Searching, screening and confiscation'

· [New] DfE (2023) 'Generative artificial intelligence in education'

· Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'

· UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

· National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

Educating pupils about online safety:
Pupils will be taught about online safety as part of the curriculum National Curriculum computing programmes of study.

From September 2020 all secondary schools have to teach:

- Relationships and sex education and health education This new requirement includes aspects about online safety.

In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity How to report a range of concerns.

By the end of secondary school, they will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online.
- The impact of viewing harmful content.
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail How information and data is generated, collected, shared and used online.
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.

The safe use of social media and the internet will also be covered in other subjects where relevant. The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Online Safety Roles and Responsibilities

The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety.

The Governor who oversees online safety is **Lynne Davies.** Our Online Safety Lead is **Karen Hagenaars.** LSA's Designated Safeguarding Lead is **Nigel Cross.**

All Governors will ensure that:

- they have read and understand this policy
- this policy is effective and complies with relevant laws and statutory guidance.
- the DSL's remit covers online safety.
- This policy is reviewed on an annual basis.
- their own knowledge of online safety issues is up-to-date.
- all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- there are appropriate filtering and monitoring systems in place.
- all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- where necessary, teaching about safeguarding, including online safety, is adapted for all students, taking into account age, SEND and other relevant factors

The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead

Details of the school's DSL and Deputy DSLs are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for all safety and this includes online safety, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, ICT manager, Year Leaders and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on CPOMS and dealt with appropriately in line with the school behaviour policy
- Ensuring there is annual staff training on online safety
- Liaising with other agencies and/or external services if necessary

The Business Manager with responsibility for Facilities and I.T.

Has responsibility for ensuring the following:

- Maintaining an appropriate level of security protection procedures, such as the Smoothwall filtering and firewall system, which are reviewed and updated on a regular basis to ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring daily reports are created by IT team and shared with pastoral staff
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly (using SOPHOS Anti- Virus)
- Ensuring the blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

The Internet Safety Lead

Has responsibility for:

- Writing and updating the Online Safety Policy and advising of necessary updates/ recommendations to our practice
- Auditing the curriculum and ensuring that we deliver the appropriate elements of Internet Safety Education within the Personal Development and ICT Curriculum. (Liaising with the Head of ICT and the Head of PSHE and other Heads of Department as appropriate.)

- Creating/Sourcing appropriate teaching resources on online safety
- Organising events around Online Safety Week and regularly throughout the year
- Running and supporting the pupil team of **Online Safety Ambassadors**, meeting regularly with them, planning events and ensuring they are supported in keeping internet safety as a high profile issue for our students, staff and parents
- Supporting parents through regular communication via newsletters, e mails and the annual production of an Online Safety Guide

ICT technicians

ICT will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
-

All staff and Volunteers

All staff, including contractors, agency staff, and volunteers are responsible for:

- Reading and understanding this policy
- Implementing this policy consistently
- Taking part in annual online safety training
- Ensuring that students follow LSA's rules on acceptable use of the internet
- Taking responsibility for the security of ICT systems and electronic data they use or have access to
- Modelling good online behaviours.

- Maintaining a professional level of conduct in their personal use of technology
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online
- Ensure that any online safety concerns are logged on CPOMS and dealt with appropriately
- Ensuring that any incidents of cyber-bullying are reported on CPOMS in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment both online and offline, reporting them to the DSL on CPOMS

Pupils

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

Parents

The LSA school website supports parents by providing useful links on online safety. The Online Safety Lead will raise parents' awareness of internet safety in an annual *Online Safety Guide*, regular newsletters and other e mails/information via MyEd. This policy will also be shared with parents and made available on LSA's website.

If parents have any queries or concerns in relation to a specific online safety incident, these should be raised in the first instance with your child's Year Leader.

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

More general enquiries about online safety should be directed to Karen Hagenaars Online Safety Lead. Karen.hagenaars@lythamhigh.lancs.sch.uk

Cyber-Bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the intentional harming of one person or group by another person or group, either one-off or repetitive, where the relationship involves an imbalance of power.(See also the anti-bullying policy)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others through PSHE delivered in Personal Development lessons.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy. When cyber bullying is reported to staff, this will be recorded on CPOMS.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Where appropriate the DSL will involve the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

This policy should be read alongside line LSA's Safeguarding, Child Protection and Behaviour Policies.

Policy written by G Clegg May 2023