Leigh Academy
Online Safety Policy

Document title:	Online Safety Policy
Version number:	1.7
Policy Status	Approved
Date of Last Review	September 2025
Date to be revised	September 2026 - This policy to be reviewed at least annually to reflect any changes to KCSIE guidance or to reflect a systemic response to significant incidents.

1 Policy statement

1.1 Vision, mission and values

We are committed to creating a positive culture of online and offline behaviours, where all pupils feel valued and welcome, supporting student learning and success. Underpinning this policy is our commitment to empowerment, respect and care for all students and staff.

Our Trust mission is to deliver "education for a better world" by ensuring that young people in our academies have an excellent start in life, regardless of their background or ability. At the centre of our mission is our commitment to safeguarding. Our vision is for all children, young people and adults to feel safe, and for anyone who works within our organisation to share this responsibility.

In addition, to ensure that all members of our community enjoy a positive, safe, and enriching online experience set within the specific context and ethos of each of our academies. We expect pupils and all stakeholders to contribute positively to the common good and uphold our expectations when online. We aim to achieve and maintain positive and responsible online behaviours. We take a firm approach to all forms of online and offline bullying and discrimination across our academies.

1.2 Purpose and intent

This policy should be read alongside the relevant policies relating to safeguarding of children which is found in the Safeguarding section of our Website and in addition to the associated statutory legislation and guidance. This policy applies to all members of the Leigh Academies Trust. This includes staff and pupils, volunteers, parents/carers, visitors, and community users who have access to and are users of the Trust's digital technology systems. All local systems adopted in our academies for managing online safety, including (but not exclusively) those incidents involving cyber-bullying and child-on-child sexual harassment and abuse, are centred on achieving a positive climate for learning and a respectful, secure culture for all children. We recognise that poor online safety and dangerous or unhealthy online habits, especially if left unaddressed, can have adverse effects on individuals, both perpetrator and victim; it can create a barrier to learning and have serious consequences for social, emotional, and mental wellbeing.

We recognise that online safety is an essential element of safeguarding, and each academy duly acknowledges its statutory obligation to ensure that all learners and staff are protected from potential online harm.

This policy supports academies in meeting statutory requirements as per the DfE guidance under the latest *DfE Keeping Children Safe in Education (2025) including Plan technology for your school* , *Working Together to Safeguard Children (2023)* and non-statutory guidance, *teaching online safety in academies (updated 2023).*

Defining online abuse: “Online abuse is any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones” (*NSPCC, 2019*). We recognise that effective, timely and robust online safety is fundamental to protecting children and young people in education and it is a significant part of the safeguarding agenda. We recognise that education has a vital role to fulfil in protecting children and young people from forms of online abuse whilst demonstrating a concerted obligation to respond with haste and flexibility to concerns as they arise.

Safeguarding children from online harm and abuse is everyone’s responsibility in our Trust. We recognise the latest data from IWF (2021) that confirms that the vast majority of self-produced sexual imagery shared online is from girls in the 11-13 age range, but the fastest growing area is amongst 7–10 year olds. This presents a particular challenge for both our primary and secondary phases.

Types of online abuse may include:

- Cyberbullying
- Emotional abuse
- Grooming
- Sexting
- Sexual abuse
- Sexual exploitation

The types, patterns and different circumstances of significant harm and abuse should be considered within the categories identified for children in the Children Act 1989/2004.
These are:

- Neglect
- Sexual
- Physical
- Emotional

We believe that the internet and associated devices are an integral part of everyday life.

We affirm that all learners should be empowered to build resilience and to develop strategies to recognise and respond to online risks.

Technology can facilitate a world of learning and development in addition to helping yield a range of opportunities. However, the stark reality is that it can also present a window to potential and actual harm and abuse. It can elicit and support an array of illegal abusive behaviours including, but not limited to:

- Harassment
- Stalking
- Threatening behaviour

- Creating or sharing child sexual abuse material
- Inciting a child to sexual activity
- Sexual exploitation
- Grooming
- Sexual communication with a child
- Causing a child to view images or watch videos of a sexual act

Current threats include the significant increase in live streaming (of sexual behaviours), coercion between minors, the sharing of nude and semi-nude images and the growth of chat sites. We commit to remaining aware of developments in social media and specific threats to childhood from the multitude of platforms. This includes:

- Misinformation
- Disinformation (including fake news)
- Conspiracy theories

These threats are exacerbated by AI and the various devices that use AI such as Smart Watches, specialised eye wear and ear pieces.

Artificial Intelligence in School

AI technology is developing rapidly, and these tools will only become more sophisticated over time. For example, they'll be able to create more convincing images or videos.
Some AI tools are not caught by filtering and monitoring systems, and can be used to generate inappropriate content that should otherwise be filtered. The Leigh Academies Trust adheres to the guidelines and expectations of the Government guidance: The Children's Commissioner's view on artificial intelligence (AI). and Using AI in education settings: support materials

As a Trust we acknowledge that AI can impact other safeguarding issues:

- Hacking and scams – text-generation tools can write convincing emails and text messages to trick pupils into giving malicious actors access to their accounts
- AI-generated child sexual abuse images – some text-to-image tools or image-altering apps (often called 'nudifying' apps) could be used to create child sexual exploitation material for sexual gratification or as a means of bullying another pupil
- 'Deepfake' pornography – superimposing a person's face into pornographic videos for sexual gratification or to humiliate the person being put in the images. AI technology is used to alter the person's facial expressions to make the video look more convincing
- 'Catfishing' and 'sextortion' – criminals can use AI-generated profile pictures to appear younger than they are to befriend and groom children and young people, and then solicit information and/or images from them (e.g. nude or semi-nude photos). They can then use this to extort children into giving them money
- Fake news and misinformation – text-to-image tools can be used to create convincing

fake photos of world events, which could be used to promote certain beliefs (including hateful ones)

- AI chatbot relationships – some AI tools allow children to chat and build a relationship with a fake person. These relationships can become very intense, and the AI may make dangerous or inappropriate suggestions

To enhance our already existing Safeguarding systems to include the additional risks that AI may bring, we encourage all staff to:

- Become more educated about AI, including the names and key uses of the main platforms and tools
- Teach about AI in the curriculum and in assemblies
- Speak to the DSL or Smoothwall if you think anything is slipping past the academy's filtering and monitoring systems
- Adhere to the Academy's Safeguarding Policy, Government Guidance "Generative AI: product safety expectations" along with due regard to KCSIE 2025

2 Roles and responsibilities

It is imperative that a whole Leigh Academy Ebbsfleet community approach to online safety is adopted and that all stakeholders are aware of their responsibilities and duties in relation to keeping children safe online. This policy will support a robust online safety ethos and ensure that academies are providing the best online safety provision they can.

The Trust board is responsible for ensuring that all pupils can access full time education and are safeguarded from harm or any sort of abuse. This is delegated to governors at a local level to provide appropriate support and challenge to senior leaders, ensuring that there is an appropriate and effective response to contextual concerns and risks, including online threats.

Senior leaders work together with the Executive team to implement this, and other associated policies into practice in the academy ensuring every child can learn in a positive and supportive environment.

The following section outlines the online safety roles and responsibilities of all stakeholders across the Leigh Academies Trust.

2.1 Trustees and governors

- Our Trust and Community Boards ensure through delegation and robust strategic scrutiny that the respective academy leadership team:
- Upholds online safety as a safeguarding issue which is embedded across the whole academy's culture
- Ensures that children are provided with a safe environment in which to learn and develop
- Ensures that the academy has filters and monitoring systems in place

- Ensures the academy has effective policies and training in place
- Ensures that risk assessments are conducted on the effectiveness of filtering systems
- Audits and evaluates online safety practice with the designated safeguarding lead and online safety lead
- Ensures there are robust reporting channels via implementation and understanding of the safeguarding policy
- Ensures that online checks are conducted and recorded on shortlisted and appointed personnel via the safer recruitment guidance in KCSIE (Keeping Children Safe in Education)

2.2 Principals (with the support of the Academies Directors, Chief Infrastructure Officer and Safeguarding Advisor):

Delegate responsibility for ensuring the academy meets its duty in delivering effective online safety to designated staff including the Online Safety Lead, cluster leads for IT, and Designated Safeguarding Lead.

Through delegation, awareness training and regular monitoring they will:

- Ensure children and young people are being appropriately taught about and know how to use the internet responsibly
- Understand and quality assure the systems that runs through Online Safety, from curriculum through to pupil voice, and the way the academy addresses child-on-child online abuse and behaviours
- Clearly signpost online safety across the respective academy curriculum
- Ensure teachers and parents are aware of measures to keep children safe online through relevant training provision
- Take responsibility for all safeguarding matters, including online safety
- Collaborate with the senior leadership team and the online safety lead
- Facilitate effective record keeping and the reporting and monitoring of all online safety concerns
- Promote online safety and the adoption of a whole academy approach
- maintain their own training and learning needs, ensuring they are up to date with all matters relating to online safety
- Ensure provision of robust filtering, monitoring, policies and practices as part of induction and ongoing training provision
- Facilitate the designated safeguarding leads and the member of staff with responsibility for online safety completion of the Trust online safety accredited training which is provided to us by KCC
- Provide up to date online safety training at least annually or more in line with legislative and statutory changes and/or in response to online safety incidents arising
- Ensure training includes recognition of risks and responses to concerns
- Inform stakeholders about monitoring and filtering processes
- Make staff aware that their online conduct outside of work can impact upon their

professional role and responsibilities

Provide advice to staff and signpost to useful resources:

- Ensure that all staff are aware of procedures to follow in recognising, responding to, and reporting online safety concerns
- Ensure that the academy operates in accordance with the UK gov guidance 'Meeting Digital and Technology Standards in Schools'
- Ensure that our key online safety and safeguarding personnel work with the local Safeguarding Partners, where suspected online abuse of minors has occurred

2.3 Teachers and other staff

All members of Leigh Academies Trust staff (teaching and non-teaching) have a responsibility to protect children online. This includes all members of staff who work within our Trust regardless of role. All staff must always act following their own professional boundaries, upholding professional behaviour and conduct at all times.

All staff need to:

- Be aware of and adhere to all academy policies which support online safety and safeguarding
- Contribute to policy development and review
- Support in the ownership of, and responsibility for, the security of systems and the data accessed
- Model good practice and appropriate behaviours when using technology – both in school and outside
- Know the process for making referrals and reporting concerns
- Know how to recognise, respond to, and report signs of online abuse and harm
- Receive child protection awareness updates on online threats and safeguarding
- Always act in the best interests of the child
- Be responsible for their own continuing professional development in online safety
- Understand that Safeguarding recording, necessitates a high standard of language, and objective reporting

2.4 Children and young people

With respect to online safety in our academies, children need to:

- Know who the DSL (Designated Safeguarding Lead) and online safety lead teacher are
- Engage in age-appropriate online safety education opportunities
- Contribute to local academy policy and curriculum development and review
- Read and adhere to local academy online safety policy appendices
- Respect the feelings of others, both off and online
- Take responsibility for keeping themselves and others safe online
- Know where and how to find help with any online incidents or concerns

- Know how, when, and where to report concerns and when to seek help from a trusted adult

2.5 Parents and Carers

We are committed to enabling parents and carers to understand the risks that children face online to protect them from online dangers. Parents should be encouraged via communication from respective academies to:

- Read and adhere to all relevant policies, including Acceptable Use expectations
- Be responsible when taking photos/using technology at academy events
- Know who their child's academy DSL is
- Know how to report online issues to the academy in the first instance
- Support online safety approaches and education provision for their child(ren)
- Be a role model for safe and appropriate behaviour
- Identify changes in their child(ren's) behaviour that could indicate they are at risk of online harm or abuse

3 Benefits of the policy

Every child will be safe and free from bullying and discrimination, enabling them to learn and thrive in an orderly, respectful, and purposeful learning environment leading to positive outcomes. All academies will have a school culture which celebrates positive learning and acknowledges respectful relationships at all levels.

4 Education and Training

Effective online safety provision and promotion of the welfare of children and young people rely upon constructive relationships that enable robust multi-agency partnership working. This can only be effective when all staff are knowledgeable, confident, and equipped with the skills to deal with processes and procedures when concerns arise relating to online abuse or harm.

We follow the principles outlined in the non-statutory guidance *'Teaching Online safety in Schools, Jan 2023'*. The Leigh AcademiesTrust is committed to the importance of educating young people on the harmful effects of online behaviours relating to child-on-child sexual abuse and harassment. The policy statement should be read in conjunction with our approach to this emerging national agenda, the guidance found in KCSIE 2025. The Leigh Academy Trust remains committed to ensuring high quality accreditation. This is a multi-step process which includes in-house and external 360 degree scrutiny and outside learning opportunities via Kent County Council. This is in conjunction with ensuring updated staff knowledge of up-to-date policies and procedures. As a Trust, we are dedicated to keeping ahead of the ever-changing online world, through ongoing learning and supporting staff in accessing resources, advice, and information from the IWF (Internet Watch Foundation) when a concern or disclosure relates to suspected online sexual abuse. Our Trust promotes and expects robust governance arrangements and collaborative practices. In accordance with KCSIE 2025, our governors and

staff receive specific training around understanding the purpose of Smoothwall which is the filtering and monitoring system used across the Trust.

Our staff recognise that online risks usually fall under one of 4 categories:

- **Contact:** Contact from someone online who may wish to bully or abuse the child. This could also include online grooming, online harassment, or activities of a commercial nature, including tracking and harvesting person information.
- **Content:** Inappropriate material available to children online including adverts, spam, sponsorship, personal info, violent or hateful content, pornographic or unwelcome sexual content, biassed materials, racist materials, and misleading information or advice.
  Conduct: The child may be the perpetrator of activities including illegal downloading, hacking, gambling, financial frauds, bullying or harassing another child. They might create and upload inappropriate material or supply misleading information or advice.
- **Commerce:** Commerce is about the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly. Schools should also consider how the risk from commerce applies to staff.

4.1 Curriculum

Each academy has a bespoke, relevant curriculum which supports online safety. We ensure each pupil receives education on safe and responsible use of and access to the internet through respective IT and wider PD (Personal Development) curriculum content, including online safety in personal, social, health and economic (PSHE) education, relationships and sex education (RSE), and information computer technology studies (ICT).

Overview of Online Safety Curriculum:

In Early Years Foundation Stage and Key Stage 1:

- Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.

In Key Stage 2:

- Learners will use age-appropriate search engines and online tools.
- Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.

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

The academies within the Leigh Academies Trust will aim to equip children and young people for digital life. Staff will promote safe and responsible internet use through teaching covering aspects of:

Age restrictions

- Explaining that age verification exists and why some sites require a user to verify their age, for example, online gambling and purchasing of certain age restricted materials such as alcohol
- Explaining why age restrictions exist, for example, to provide a warning that the site may contain disturbing material that is unsuitable for younger viewers
- Helping pupils to understand how this content can be damaging to under-age consumer
- Explaining what the age of digital consent means - the minimum age (13) at which young people can agree to share information and sign up to social media without parental consent under General Data Protection Regulations
- How content can be used and shared
- What happens to information, comments or images that are put online.
- What a digital footprint is, how it develops and how it can affect future prospects such as university and job applications
- How cookies work
- How content can be shared, tagged, and traced
- How difficult it is to remove something a user wishes they had not shared.
- the risk of identity theft or targeted approach from fraudsters using information shared online
- Ensuring pupils understand what is illegal online, for example: youth-produced sexual imagery (sexting) sharing illegal content such as extreme pornography or terrorist content the illegality of possession, creating or sharing any explicit images of a child even if created by a child

Disinformation, misinformation, and hoaxes

Some information shared online is accidentally or intentionally wrong, misleading, or exaggerated.
Teaching may include:

- Disinformation and why individuals or groups choose to share false information to deliberately deceive
- Misinformation and being aware that false and misleading information can be shared inadvertently
- Malinformation and understanding that some genuine information can be published with the deliberate intent to harm, for example releasing private information or photographs

(including revenge porn)
- Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons
- Explaining that the viral nature of this sort of content can often appear to be a stamp of authenticity and therefore why it is important to evaluate what is seen online
- How to measure and check authenticity online
- The potential consequences of sharing information that may not be true

AI Hallucinations

AI hallucination is a phenomenon where a generative AI chatbot or computer vision tool, perceives patterns or objects that are nonexistent or imperceptible to human observers, creating outputs that are nonsensical or altogether inaccurate.

Preventing AI hallucinations

The best way to mitigate the impact of AI hallucinations is to stop them before they happen. Here are some steps to keep AI models functioning optimally:

- Use high-quality training data
- Use data templates
- Limit responses
- Test and refine the system continually

Fake websites and scam emails

Fake websites and scam emails are used to extort data, money, images, and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or another gain.

Teaching may include:

- How to look out for fake URLs and websites
- Ensuring pupils understand what secure markings on websites are and how to assess the sources of emails
- Explaining the risks of entering information to a website which is not secure
- What to do if harmed, targeted, or groomed as a result of interacting with a fake website or scam email
- Who to go to and the range of support that is available
- Explaining the risk of ‘too good to be true’ online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist

Fraud (online)

Fraud can take place online and can have serious consequences for individuals and organisations.

Teaching may include:

- What identity fraud, scams and phishing are
- Explaining that online fraud can be highly sophisticated and that anyone can be a victim
- How to protect yourself and others against different types of online fraud
- How to identify ‘money mule’ schemes and recruiters
- The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal
- The risk of sharing personal information that could be used by fraudsters
- Explaining that children are sometimes targeted to access adults’ data, for example, passing on their parent or carer’s bank details, date of birth or national insurance number
- What good companies will and will not do when it comes to personal details, for example, a bank will never ask you to share a password or move money into a new account
- How to report fraud, phishing attempts, suspicious websites, and adverts

Password phishing

Password phishing is the process by which people try to find out your passwords so they can access protected content.

Teaching may include:

- Why passwords are important, how to keep them safe and that others may try to trick you to reveal them
- Explaining how to recognise phishing scams, for example, those that try to get login credentials and passwords
- The importance of online security to protect against viruses (such as keylogging) that are designed to access, steal, or copy passwords.
- What to do when a password is compromised or thought to be compromised

Personal data

Online platforms and search engines gather personal data. This is often referred to as ‘harvesting’ or ‘farming.’

Teaching may include:

- How cookies work
- How data is farmed from sources which look neutral, for example, websites that look like games or surveys that can gather lots of data about individuals
- How, and why, personal data is shared by online companies, for example, data being resold for targeted marketing by email and text (spam)
- How pupils can protect themselves, including what to do if something goes wrong (for example data being hacked) and that acting quickly is essential
- The rights children have regarding their data, including protections for children under the General Data Protection Regulations (GDPR)
- How to limit the data companies can gather, including paying particular attention to boxes

they tick when playing a game or accessing an app for the first time

Persuasive design

Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Some AI chatbots can be very convincing, especially to children. Children can start to treat chatbots like a trusted friend, and older children may discuss romantic/sexual topics or convince them to commit crimes. These relationships with chatbots can have significant negative effects on mental health and wellbeing.

Teaching may include:

- Explaining that most games and platforms are businesses designed to make money - their primary driver is to encourage users to be online for as long as possible to encourage them to spend money (sometimes by offering incentives and offers) or generate advertising revenue.
- How designers use notifications to pull users back online

Privacy settings

All devices, websites, apps, and other online services come with a privacy setting that can be used to control what is shared.

Teaching may include:

- How to find information about privacy setting on various sites, apps, devices, and platforms
- Explaining that privacy settings have limitations, for example, they will not prevent someone posting something inappropriate

Targeting of online content (including on social media and search engines)

Much of the information seen online is a result of some form of targeting.

Teaching may include:

- How adverts seen at the top of online searches and social media feeds have often come from companies paying to be on there and different people will see different adverts
- How the targeting is done, for example, software which monitors online behaviour (sites they have visited in the past, people who they are friends with) to target adverts thought to be relevant to the individual user
- The concept of clickbait and how companies can use it to draw people onto their sites and services We support learners' understanding based on age and ability through:
- 'Acceptable Use' posters in all rooms with internet access
- Informing all learners of monitoring and filtering that is in place
- Implementing peer education strategies • providing continuous training and education as part of their transition across key stages • using alternative, complementary support

where needed
- Seeking pupil voice.

Large language models (LLMs)

Large language models (LLMs) are a category of foundation models trained on immense amounts of data making them capable of understanding and generating natural language and other types of content to perform a wide range of tasks. LLMs are designed to understand and generate text like a human, in addition to other forms of content, based on the vast amount of data used to train them. We promote Safeguarding by ensuring access to AI tools and technology that is trustworthy, transparent, responsible and secure.

4.2 Vulnerable learners

Vulnerable children who need our help the most are not only missing opportunities to flourish online but are often experiencing the very worst that the online world can be. We recognise that some learners are more vulnerable due to a range of factors.

Those children may:

- Receive statutory care or support
- Have Special Educational Needs and Disabilities
- Have experienced specific personal harm
- Have a disability, be experiencing ill-health, or developmental difficulties
- Live in households or families with characteristics or locations that indicate higher potential likelihood of current and future harm
- Live in households where domestic abuse, parental substance abuse or mental health issues are present • be vulnerable or of concern by virtue of their identity or nationality
- Be at risk in relation to activity or institutions outside the home
- Be a Young Carer

We will ensure the effective and safe provision of tailored online safety education for such pupils on a bespoke package, which augments the general academy offer. We will seek input and advice from specialist staff or appropriate outside agencies as necessary.

5 Cultivating a safe environment

"All staff should be aware of indicators which may signal that children are at risk from, or are involved with, serious violent crime. These may include increased absence from academies, a change in friendships or relationships with older individuals or groups, a significant decline in performance, signs of self-harm or a notable change in well-being, or signs of assault or unexplained injuries. Unexplained gifts or new possessions could also indicate that children have been approached by, or are involved with, individuals associated with criminal networks or gangs" (DfE, 2019).

The online world is increasingly used as a platform for the above.

Children in will be educated in an age-appropriate way about:

- How to evaluate what they see online
- How to recognise techniques for persuasion
- Their online behaviour
- How to identify online risks
- How and when to seek support

5.1 Evaluate – how to evaluate what pupils see online

This will enable our students/pupils to make judgments about what they see online and not automatically assume that what they see is true, valid, or acceptable. We work to challenge the increasing challenges that come with Artificial intelligence (AI) systems taking on human biases and amplifying them through our Safeguarding Curriculum and Staff Unconscious bias training. Leigh Academies Trust will help students/pupils to consider questions including (but not exclusively):

- Is this website/URL/email fake? How can I tell?
- What does this cookie do and what information am I sharing?
- Is this person who they say they are?
- Why does someone want me to see this?
- Why does someone want me to send this?
- Why would someone want me to believe this?

5.2 Recognise – how to recognise techniques used for persuasion

This will enable pupils to recognise the techniques that are often used to persuade or manipulate others. A strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biassed intent or malicious activity.

We help pupils to recognise:

- Online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation)
- Techniques that companies use to persuade people to buy something
- Ways in which games and social media companies try to keep users online longer (persuasive/sticky design)
- Criminal activities such as grooming

5.3 Online behaviour expectations

We expect that this section is read in conjunction with the Trust's Behaviour and Anti-Bullying policies. This will enable staff to educate our pupils in understanding what acceptable and unacceptable online behaviour looks like. We teach children that the same standard of behaviour and honesty applies online and offline, including the importance of respect for others. We also

teach them to recognise unacceptable behaviour in others.

We help pupils to recognise acceptable and unacceptable behaviour by:

- Looking at why people behave differently online. For example, how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do
- Looking at how online emotions can be intensified resulting in mob mentality
- Teaching techniques (relevant on and offline) to defuse or calm arguments (for example, a disagreement with friends) and disengage from unwanted contact or content online
- Considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming, and the acceptance of misogynistic, homophobic, and racist language that would never be tolerated offline.
- Provide greater understanding that misinformation is accidental, disinformation is the deliberate creation or spreading of false information.
- Ensure that students know that Text-to-image AI generators can create convincing fake images of world events and Extremists can use these fake images and news stories to push their own hateful beliefs
- To understand that AI isn't perfect and will make mistakes even when it's not being used maliciouslY

5.4 Identify – how to identity online risks

This will enable our staff to educate students/pupils in identifying possible online risks and make informed decisions about how to act. The focus is to help our children assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

We help children to identify and manage risk by:

- Discussing the ways in which someone may put themselves at risk online
- Discussing risks posed by another person's online behaviour
- Discussing when risk taking can be positive and negative
- Discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations, i.e., how past online behaviours could impact on their future when applying for a place at university or a job
- Discussing the risks versus the benefits of sharing information online and how to make a judgement about when and how to share, and who to share with
- Asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

5.4.1 Online radicalisation

We recognise that children, young people, and adult learners are at risk of accessing inappropriate and harmful extremist content online. This could include downloading or sharing terrorist material, which could be a criminal act. The internet and social media make spreading divisive and hateful narratives easier. Extremist and terrorist groups and organisations use social

media (for example, apps, forums, blogs, chat rooms) to identify and target vulnerable individuals.

Our teaching will include:

- How to recognise extremist behaviour and content online • understanding actions which could be identified as criminal activity
- Exploring techniques used for persuasion
- Knowing how to access support from trusted individuals and organisations We have a responsibility under the Prevent duty which includes building our students' resilience to extremism and ensuring staff are adequately trained to spot the signs of radicalisation.

5.4.2 Fake profiles

We recognise that not everyone online is who they say they are.

Teaching will include:

- Explaining that in some cases profiles may be people posing as someone they are not (such as an adult posing as a child) or may be bots (which are automated software programs designed to create and control fake social media accounts)
- How to look out for fake profiles, for example: profile pictures that do not like right accounts with no followers or thousands of followers a public figure who does not have a verified account

5.4.3 Grooming

As part of our wider safeguarding duty, we expect designated staff and pupils in our academies to know about the different types of grooming and motivations for it, for example:

- Radicalisation
- Child sexual abuse and exploitation
- Gangs (county lines)
- Financial exploitation (money mules)

Teaching will include:

- Boundaries in friendships with peers, families and with others
- The key indicators of grooming behaviour
- Explaining the importance of disengaging from contact with suspected grooming and telling a trusted adult
- How and where to report it both in school, for safeguarding and personal support, and to the police

5.4.4 Live streaming

We recognise that live streaming (showing a video of yourself in real-time online either privately or to a public audience) can be popular with children but it carries risk when carrying it out and

watching it.

Teaching will include:

- Explaining the risks of carrying out live streaming such as the potential for people to record live streams without the user knowing and content being shared without the user's knowledge or consent
- That online behaviours should mirror offline behaviours and considering any live stream in that context - pupils should not feel pressured to do something online that they would not do offline
- Explaining the risk of watching videos that are being live streamed, for example, there is no way of knowing what will come next and so this poses a risk that a user could see something that has not been deemed age appropriate in advance
- Explaining the risk of grooming

5.4.5 Indecent Images/material/Pornography

We understand and communicate that sexually explicit material presents a distorted picture of sexual behaviours. The teaching of this aspect of online safety is in conjunction with our wider safeguarding duty.

Teaching will include that:

- Pornography is not an accurate portrayal of adult sexual relationships
- Viewing pornography can lead to skewed beliefs about sex and in some circumstances can normalise violent sexual behaviour
- That not all people featured in pornographic material are doing so willingly, such as revenge porn or people trafficked into sex work This content is covered as part of the relationships and sex education core content (secondary).

5.4.6 Unsafe communication

Our pupils should know different strategies for staying safe when communicating with others, especially people they do not know or have never met.

Teaching will include:

- Explaining that communicating safely online and protecting your privacy and data is important regardless of who you are communicating with
- Identifying indicators of risk and unsafe communications
- Identifying risks associated with giving out addresses, phone numbers or email addresses to people you do not know or arranging to meet someone you have not met before
- Explaining about consent online and supporting pupils to develop strategies to confidently say "no" to both friends and strangers online

5.5 How and when to seek support

This will enable staff to support students/pupils in understanding safe ways in which to seek support if they are concerned or upset by something they have seen online.

The Leigh Academies Trust will:

- Help them to identify who trusted adults are
- Look at the different ways to access support from police, the National Crime Agency's Click CEOP reporting service for children, Internet Watch Foundation (IWF), National Online Safety, and organisations, such as Childline.

This policy links to the wider Trust policies and processes around reporting of safeguarding and child protection incidents and concerns to academy staff (see the current iteration of Keeping Children Safe in Education)
help them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported

6 Responding to online safety concerns

Any concern that children and young people may be at risk of harm or abuse must immediately be reported. The DSL takes the lead responsibility for online safety concerns, which are initially recorded and actioned using Bromcom. Children and young people will be enabled (at a level appropriate to their age and ability) to share online concerns.

Remember:

- Child welfare is the principal concern – the best interests of children always take precedence over GDPR and any other restriction that may present itself
- If there is any immediate danger, contact the police on 999
- Refer to all agencies as per Leigh Academies Trust local safeguarding processes.
- Always adhere to local safeguarding procedures and report to the DSL and principal within each academy – who will then act

7 Responding to complaints

There are several sources from which a complaint or allegation might arise, including those from:

- A child or young person
- An adult.
- A parent/carer.
- A member of the public (including a friend or relative).
- A colleague.

There may be up to three components in the consideration of an allegation:

- A police investigation of a possible criminal offence.

- Enquiries and assessment by children's social care or adult social care relating to whether a child, young person or adult at risk needs protection or services.
- Consideration by an employer of disciplinary action in respect of the individual (including suspension)

8 Monitoring, filtering, and compliance

In adhering to the revised guidance on filtering and monitoring in KCSIE 2025, the Trust uses the Smoothwall Filtering and Monitoring. DSLs (Designated Safeguarding Leads) may use this to view alerts for safeguarding violations and review and action the critical and urgent alerts. Smoothwall also provides an overview of all violations across an academy.

DSLs, in accordance with KCSIE 2025, have an ongoing monitoring of the Filtering & Monitoring systems within their academy. Any checks completed are recorded on a tracker where contextual themes can be identified and inform staff/pupil training.

9 The Online Safety Bill 2023

We always adhere to the online safety section of Keeping Children Safe in Education, which addresses key themes within the Bill.

The Bill primarily protects children, by imposing a duty on user-to-user service providers to:

- Remove harmful content or ensure that it does not appear in the first place
- Enforce age limits and age-checking measures
- Ensure risks and dangers to children's safety are more transparent, including publishing risk assessments

Any platform that is likely to be accessed by children will now have a duty of care, which means the providers must take steps to protect children and young people from accessing content that is illegal and harmful. Some content, while not illegal, may be harmful or age-inappropriate for children.

Our Trust is alert to the impending legal guidance outlined in the Online Safety Bill. For our academies, the safeguarding duties will remain the same. The Bill will not remove our responsibility or mean safeguarding children and young people online is put into the hands of third parties.

10 Misuse

The Internet, Intranet, email, messaging systems and related technologies must not be used for knowingly viewing, communicating, retrieving, downloading or storing any communication that is:

- Discriminatory or harassing;
- Derogatory to any individual or group;
- Obscene or pornographic;

- Defamatory, threatening or seen as cyber bullying;
- Illegal or contrary to LAT policy or interests;
- Subject to Copyright such as music, software or films;
- Likely to cause network congestion or significantly hamper access for other users;
- Any of the above, specifically using mobile devices or similar technologies to store or upload any such materials to the public domain (social networking sites) or to other devices;

Except in cases in which explicit authorisation has been granted by LAT Executive team, users are prohibited from engaging in, or attempting to engage in:

- Monitoring or intercepting the files or electronic communications of other users;
- Using another user's log-ins or passwords;
- Breaching, testing, or monitoring computer or network security measures;
- E-mail or other electronic communication that attempts to hide the identity of the sender or represent the sender as someone else;
- Hacking, Blue-jacking or accessing systems or accounts that they are not authorised to use;
- Obtaining electronic access to other companies' or individuals' materials. (Copyright means users cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner).

Law and LAT policy prohibits the theft or abuse of computing resources and includes:

- Unauthorised entry;
- Using, transferring and tampering with other people's accounts and files;
- Interfering with other people's work or computing facilities;
- Sending, storing or printing offensive or obscene material including content that may be
- interpreted as sexual or racial harassment;
- Mass mailing of messages;
- Internet use for personal commercial purposes;
- Using the Internet/intranet facilities or equipment to deliberately propagate any virus, worm, Trojan horse or any such other programme that is harmful to normal computer operations;
- Accessing or uploading to any obscene or pornographic sites. Sexually explicit material may not be viewed, archived, stored, distributed, edited or recorded using the Academy's networks or computing resources; If a user finds himself/herself connected accidentally to a site that contains sexually explicit or offensive material, they must disconnect from that site immediately. Such unintentional access to inappropriate internet sites must be reported immediately to the respective tutor, line manager or Principal. Any failure to report such access may result in disciplinary action.

It is impossible to define all possible unauthorised use, however, disciplinary action may be taken where a user's actions warrants it.

Other actions deemed unacceptable, although not exhaustive, include:

- Theft or copying, sharing of files without permission;
- Sending, sharing or posting the LAT or other stakeholders confidential files outside of the organisation or inside the organisation to unauthorised staff, students or other users;
- Refusing to cooperate with reasonable security investigation.

11. Passwords

With the advent of increasingly sophisticated password cracking programs, steps need to be taken to minimise the problem posed by malicious users trying to break into accounts. Therefore, wherever possible, two factor authentication (2FA) will be enabled. The security of passwords used with accounts is a highly important issue. The passwords you use should be carefully considered as badly chosen passwords have the potential to be cracked or easily guessed.

- Passwords must be at least 8 characters long and should be a combination of letters and numbers. 'Utilising three random words (plus numbers) is a good balance between security and usability.'
- A password must not be based on anything connected with the individual who owns the account. This includes anything associated with a name or initials, job description, address or postcode.
- Any passwords generated for use by the IT Services Team should be changed immediately after initial use.
- User accounts are issued by the Trust IT Team for individual use only.
- Accounts and passwords must not be shared, given away or offered for use to anybody else.
- Users must take all reasonable steps to keep their passwords confidential and must not disclose them to anyone else.

12 . Internet Access

All access to the Internet at each Academy must be via the filtering software installed by LAT. This filtering software should help to prevent access to inappropriate sites available over the Internet. However, no automatic filtering service can be 100% effective in preventing access to such sites and it is possible that users may accidentally access unsavoury material whilst using the Internet. In such circumstances, users must exit the site immediately and advise the person responsible for IT in the academy, providing details of the site, including the web address, to reduce the possibility of the material being accessed again in future. The person responsible for IT will then arrange for the filtering rules to be revised to exclude the site.

Access to the Internet is available for authorised users only and is provided to support work related activities and for educational purposes only.
There is a huge amount of information available to users via the Internet, and students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Students should be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

13. Email, Messaging and Social Networking

Those that use the LAT e-mail, messaging or other digital communication services are expected to do so responsibly, comply with all applicable laws, other policies and procedures of LAT and with normal standards of professional and personal courtesy and conduct.

The Leigh Academies Trust follows sound professional practices to secure e-mail records, messaging systems, data and system programmes under its control. As with standard paper based mail systems, confidentiality of these cannot be 100% assured. Consequently users should consider the risks when transmitting highly confidential or sensitive information and use the appropriate level of security measure.

Enhancement of the base level security to a higher or intermediate level can be achieved by the use of passwords for confidential files. It should be remembered that messages forwarded from another individual can be amended by the forwarder. This possibility should be considered before acting on any such mail. In order to effectively manage these systems the following should be adhered to:

- Open messages/mailboxes must not be left unattended;
- Care should be taken about the content of a message as it has the same standing as a letter;
- Report immediately to IT Services via raising an IT ticket on our Trust system called Halo when a virus is suspected in a message;
- Users must not:
- Ignore messages. These systems are designed for speedy communication. If the message requires a reply, a response should be sent promptly within reasonable working hours;
- Use anonymous messaging services to conceal identity when mailing through the Internet; falsify emails to make them appear to originate from someone else, or provide false information to any Internet service which requests name, e-mail address or other details;
- Abuse others, even in response to abuse directed at them;
- Use these technologies, either internally or on the Internet, to sexually harass fellow employees, or harass or threaten anyone in any manner.

The transmission of user names, passwords, chain mail or other information related to the security of the Leigh Academies Trust computers is not permitted.
Although not allowed within the academies, we do realise that the majority of young people are using social networking sites at home. We aim to make students responsible users of these sites and therefore students should be made aware of the advantages and dangers of using these websites.

14. Media Publications

Video and photographic technologies can be very powerful learning tools. However, photographs and/or video may be taken by staff to support educational aims only. Named images of students will only be published with the separate written consent of their parents or carers. Publishing includes, but is not limited to:

- LAT websites and newsletters
- Web broadcasting,
- TV presentations
- Newspapers

Care should be taken when capturing photographs or videos to ensure that all students are appropriately dressed and permissions gained from parents and carers in line with normal guidance.

15. Use at Home

Students, staff or other users accessing the Internet from home whilst using an LAT owned computer or mobile device or through Leigh Academies Trust owned connections such as the Sophos Connect VPN client must adhere to the policies set out in this document.
Family members or other 'non-LAT' users must not be allowed to access LAT computer systems or use the LAT computer facilities. It is an expectation that Pupils using Leigh Academies Trust devices/internet systems will be supervised by an appropriate adult at home. Smoothwall Web Filtering & Monitoring tools are continuously active on a Trust device regardless of it's physical location. Any inappropriate use of devices/systems will be addressed through processes outlined in our Safeguarding and Child Protection and Acceptable Use Policies.

16. Complaints

The Leigh Academies Trust will take all reasonable precautions to ensure appropriate Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a LAT computer or mobile device. The Leigh Academies Trust cannot accept liability for material accessed, or any consequences of Internet access.
Students and staff have access to information about infringements in use and possible sanctions.
In addition to usual Academy sanctions the following may be appropriate:

- Interview or counselling by appropriate member of staff;
- Removal of Internet or computer access for a period, which could ultimately prevent access to
- Files held on the system, including staff files or student examination coursework;
- Referral to Children's Social Care/Police or other relevant authorities;

The Academy Designated Safeguarding Lead acts as the first point of contact for any complaint.

However, any complaint about staff, student or other users misuse can also be referred to the Principal.

Complaints of Cyber-bullying are dealt with in accordance with our Anti-Bullying Policy, Acceptable Use Policies and Safeguarding/Child Protection Policy. .

17. Data Protection

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government.The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).Everyone responsible for using personal data has to follow strict rules called 'data protection principles'.

They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

Any data processing or storage of personal information is dealt with in accordance with our Data protection policy.

18. Disclaimer and review

Every effort has been made to ensure that the information contained within this policy is up to date and reflective of the latest legislative and statutory guidance. The online world is fast changing, and we recognise that areas of policy may need to be adapted and amended to reflect this. If errors are brought to our attention, we will correct them as soon as is practical. This policy will be reviewed annually to reflect legislative changes or developments, to ensure its continuing relevance.

19 Further sources of information

We follow the principles outlined in the guidance 'Meeting digital and technology standards in schools and colleges, March 2023'. In addition to the above, the links below to relevant government guidance and a range of national organisations can offer support to parents and schools.

Related guidance is available on:

- relationships and sex education (RSE) and health education
- national curriculum in England computing programmes of study

National curriculum in England citizenship programmes of study Support and resources are also available from:

- the CEOP Thinkuknow Programme
- UK Council for Internet Safety
- Education for a Connected World

Our academies can also get advice from national organisations such as:

- Anti-Bullying Alliance
- Childnet 25
- Internet Matters
- Internet Watch Foundation
- NSPCC learning
- PSHE Association
- SWGfL
- UK Safer Internet Centre

Common Sense Education

Our parents may also access the following national organisations for support:

- Internet Matters
- NSPCC
- Parent Zone

Our pupils may access the following national organisations for support:

- BBC Own It
- Childline