Arthur Terry Learning Partnership

Together we are stronger

Online safety policy

Document Control

Primary Contact:	ATLP Safeguarding Team & Learning Futures Project Team safeguarding@atlp.org.uk
Version:	2.0 Previous version titled e-safety policy
Status:	Approved
Updated:	August 2023
Related Documents:	Acceptable Use policy Behaviour Policy Safeguarding and child protection policy GDPR data protection policy Social Media policy RSHE policy – primary and secondary Complaints Policy
Review Frequency:	Annually or upon legislative change
Approved/Ratified by:	Trust Board 23/10/23

Who is this policy for?

The ATLP is committed to safeguarding and promoting the physical, mental and emotional welfare of every student, which includes safeguarding children to the best of our ability in online spaces. This policy applies to all staff, students, parents/carers and suppliers of the Arthur Terry Learning Partnership, as safeguarding is everyone's responsibility.

The content of this policy applies to all devices with the capacity to connect to the internet and transfer data. This includes internet-connected toys, tablets, smart TVs and watches, phones, laptops and computers. Specific attention is paid to ATLP-provided devices. Individuals should refer to the ATLP 'Acceptable Use' or 'Bring your own device' policies as appropriate.

This policy relates to all schools within the Arthur Terry Learning Partnership (ATLP). The term 'schools' is used to refer to any school or school within the ATLP. The phrase headteacher also relates to Heads of School.

Where this policy refers to 'staff' or 'we', the policy refers collectively to all employees in the Trust, as well as agency workers, self-employed contractors and governance representatives (i.e. Trustees, Advocates and Members).

Guiding principles

At the Arthur Terry Learning Partnership ("ATLP"), children lie at the heart of everything we do. We are committed to guaranteeing that every student receives the same opportunities, addressing inequality both inside and outside of the classroom. We know that learning does not only take place in the classroom, but also at home, and that our young people's families play an important role in supporting their children with their education.

We are committed to preparing our children and young people for their next steps, ensuring that they are fully prepared for the rapidly evolving technological landscape. We recognise that technology will equip our children with the tools required for life in the future. We are committed to sharing our knowledge and expertise with students, parents and carers, safeguarding partners and other schools and MATs, so that we can continue to safeguard and promote the well-being of children and young people in our care.

We recognise that no filtering system is 100% safe. ATLP's filtering system will block internet access to harmful sites and inappropriate content for devices that are connected to ATLP networks, or provided by the Trust for staff or student use. It should not unreasonably impact teaching and learning or school administration or restrict students from learning how to assess and manage risk themselves.

The ATLP is totally committed to safeguarding the welfare and promoting the welfare of children and young people. We recognise that safeguarding is everyone's responsibility. This includes all staff, trustees and advocates. We are committed to providing a safe environment to learn, including when online. We are committed to ensuring that children and young people are safeguarded from potentially harmful and inappropriate online material.

The ATLP is committed to ensuring that all staff undergo annual safeguarding and child protection training, including training regarding online safety. Training will be in line with any advice received from the ATLP's safeguarding partners, and will include an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring. This training will be regularly updated.

We are equally committed to ensuring that we balance our duties to protecting children and young people with our responsibilities to our staff. We are committed to ensuring that all our staff have a manageable workload, and that we do our best to protect their well-being.

Roles and responsibilities

The day-to-day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. We are committed to ensuring that everyone in our organisation, as well as our external providers, understand their role in keeping our students safe online.

The Trust Board is responsible for:

- the approval of the online safety policy and for reviewing its effectiveness
- ensuring that there is a member of the Trust's leadership team and a trustee/s who are responsible for ensuring these standards are met
- ensuring that filtering and monitoring provision is reviewed, as part of a wider online safety review at least annually
- ensuring all staff and external service providers understand their roles and responsibilities in relation to online safety.
- ensuring that all staff and governance representatives have completed the Trust's annual safeguarding training requirements

School Advocates are responsible for:

- completing the Trust's annual safeguarding training requirements
- having an awareness of online threats, risks and trends in technology use and internet use.
- supporting and critically challenging their schools in local implementation and compliance with this online safety procedure and practice.

The Learning Futures Team and the Trust Safeguarding Leads are jointly responsible for ensuring that the standards for filtering and monitoring are met. This includes:

- procuring filtering and monitoring systems
- liaising with the external provider to ensure that the technical requirements to meet regulatory standards are in place
- documenting decisions on what is blocked or allowed and why
- ensuring that blocklists are reviewed and can be modified in line with changes to safeguarding risks
- is overseeing and acting on filtering and monitoring reports
- ensuring that all Hub and lead DSLs are adequately trained in the Trust's filtering and monitoring systems and maintain an overview of trends in the data
- reviewing the effectiveness of our provision, at least annually
- reporting to the Trust Board and providing assurance that systems are working effectively and meeting safeguarding obligations, and/or advising of any associated risks or incidents.
- meeting on a half-termly basis to review any risks related to the trust's online safety
- advising on online safety content for schools' PSHE curriculums.

Trust safeguarding leads will take the lead responsibility for safeguarding, including online safety. This includes overseeing and acting on safeguarding concerns.

The ATLP filtering and monitoring service provider [1]has technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports

The Trust's IT service provider and inhouse team will work jointly to:

- complete actions following concerns or checks to systems.

The Trust's IT service provider and inhouse team will work with the Learning Futures Team and Trust safeguarding leads to:

- procure & implement systems on devices
- ensuring that filtering and monitoring systems work on new devices and services before releasing them to staff and students
- identify risk
- carry out reviews
- carry out checks.

Headteachers and Heads of school are responsible for ensuring that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns, for example by ensuring that incidents are logged and reviewed within agreed timescales (see below)
- know how to report and record concerns
- understand how to deal with incidents of concern during term time
- are duly protected from dealing with any incidents outside of normal working hours.

Lead/hub DSLs are responsible, during term time, for:

- ensuring that all L3,4 and 5 incidents are responded to appropriately. This includes, for example, liaising with emergency services when there is a Level 5 threat to life
- ensuring that all level 3, 4 and 5 incidents are recorded on the school's MyConcern record
- seeking supervision on a regular basis, including when they dealt with a Level 5 threat to life concern.

All staff are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of current Trust online safety policy and practices
- they have read and understood the appropriate ATLP Acceptable Use policies
- digital communications with students are only on a professional level and carried out using official Trust systems
- students understand and follow the Trust's Online Safety and Acceptable Use Policy
- they are aware of the relevant Trust policies[2] which refer to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current best practice with regard to these devices
- in class and when using the internet, students are guided to sites that are checked as suitable for their use and that processes are in place to deal with any unsuitable material that is found in internet searches
- ensuring that user names, logins, email accounts and passwords are used effectively

[1] The ATLP e-safety service provider is currently 'Smoothwall'.

[2] ATLP Behaviour Policy, Parental Code of Conduct, Social Media Policy

- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given

All staff should make a report to the school's DSL when:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

See the actioning process in Section 5 below.

Students and parents/carers are responsible for ensuring that:

- reviewing and adhering to the ATLP 'Acceptable Use' and 'Social Media' Policies.
- Ensuring that personal details, including user names, logins, email accounts and passwords are used effectively, and shared only as appropriate.
- Ensuring personal devices are kept locked when not in use, and are password protected.
- Reporting any potential data breaches or loss of device to a member of school staff without delay.
- Demonstrating caution when accessing online platforms and material and reporting to a member of staff any instances where inappropriate material has been inadvertently accessed.

5. The 4 areas of risk

We recognise the 4 areas of risk as set out in KCSIE 2023:

Area of risk:	**How will we minimise these risks?**
content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism	We will minimise these risks through an effective filtering system that will block access to such content, and by monitoring any attempts to access such content. We will educate students about harmful online content through our RSHE programme: Primary Relationships and Health Education Policy Secondary RSE and Health Education Policy
contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other.	We will minimise this risk through an effective filtering system that will block access to harmful online content. We monitor and act on harmful online interaction between students. We will educate students about the risks of commercial advertising and adults posing as children or young people. **This includes the use of artificial intelligence to pose as a child or young person.**

conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g., consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.	We will minimise these risks by ensuring that our filtering and monitoring system will block attempts to make, send and receive explicit images such as the sharing of nudes and semi-nudes and/or pornography. It will alert us to attempts to do so. It will alert us to online bullying. We will educate students about the risks of making, sending and receiving explicit images. We educate them to understand what is meant by consent in healthy relationships.
commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.	We will minimise these risks by ensuring that our filtering and monitoring systems block access to online gambling, inappropriate advertising, phishing and or financial scams. We will educate students about such risks through our PSHE programme. When we identify that students or staff are at risk, we will put appropriate measures in place. This may include safeguarding support.

Additional technology risks

Generative artificial intelligence (AI)

The ATLP recognises that recent advances and public access to generative artificial intelligence (AI) mean that the general public can now use this technology to produce AI-generated content. This poses opportunities and challenges for schools.

Whilst the ATLP is committed to preparing our children for the tools and jobs of the future, which will include the use of AI; staff, children and parents/carers must be aware that generative AI can increase the sophistication and credibility of cyber-attacks and can also be used to access or generate harmful content. The content they produce is not always accurate or appropriate as it has limited regard for truth and can output biased information. We acknowledge the increased risk of adult-on-chilf or child-on-child abuse that AI potentially poses

All staff and students must be aware that personal and sensitive data must be protected at all times and must not be entered into generative AI tools. Any data entered into AI tools should not be identifiable and should be considered released to the internet.

Generative AI for student work is only to be used by students with the express permission of the relevant teacher and must be declared. Under no circumstances should generative AI responses be presented as a childs own work.

The use of mobile and smart technology

The ATLP recognises that many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e., 3G, 4G and 5G) and other personal devices. This access means some children, while at school, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content.

We minimise these risks by ensuring that:

- the Trust maintains effective behaviour, safeguarding and social media policies.

- Ensuring that each school has effective communication in place regarding their local expectations and rules, that make explicit the extent to which mobile phones may be used on school sites
- each school has effective anti-bullying policies in place that, in conjunction with the Trust's Behaviour Policy and Safeguarding Policies, set out clear consequences of misusing mobile phones to sexually harass, bully and control others, share indecent images consensually or non-consensually and view and share pornography or other harmful content.
- each school has in place an effective programme of PSHE that educates students about the safe and acceptable use of mobile phones and smart technology and about the benefits and risks of AI

Online safety and Learning Futures

Learning Futures is an exciting initiative to ensure that all students in the ATLP have equality of access to technology and can benefit from its capabilities to support and enhance learning at school and home.
The deployment of Learning Futures devices for use by students beyond the school needs to be carefully considered in the application of online safety best practice.

When devices are issued to students and staff, it is made clear that students enrolling their device is a sign of agreement to the ATLP Acceptable Usage Agreement.

The ATLP will ensure that parents and carers are provided with appropriate information and support to enable them to manage the risks associated with young people making use of Learning Futures devices at home.

The Trust has made the 'Jamf' Parent App [3]available to all parents and carers. This allows parents to implement some technical controls over Learning Futures devices when it is away from school. Support and guidance for parents and carers to implement and use this application will be provided.

To support screen time, applications on Learning Futures devices will disappear at 8pm – 7.30am in primary school and 10pm – 7.30am in secondary school. These times will be amended during holiday times in line with our guiding principles to protect the work-life balance of our staff. During holiday times, all apps will be switched off at 8pm.
Further limitations and restrictions can be added to student devices if a DSL feels a student is not using a device appropriately. This includes, but is not limited to, the removal of internet browsing applications.

6. Internet access, monitoring and filtering

ATLP makes use of a monitoring and filtering solution (Smoothwall) on all student and staff devices. This software will be installed, configured and managed by the ATLP IT team for all ATLP-provided devices. ATLP monitoring and filtering software will also extend to guest devices[4] connected to ATLP broadband. The software is used to monitor and filter activities undertaken on the devices, and alerts relevant staff to any safeguarding concerns. The provider monitors and categorises incidents of safeguarding concern for the attention of the school/trust.

Smoothwall is a member of the Internet Watch Foundation (IWF), the UK Safer Internet Centre and the Anti-Bullying Alliance and are signed up to the Counter Terrorism Internet Referral Unit list (CTIRU) Smoothwall will filter all internet feeds including any back-up connections.

[3] https://atlp.org.uk/about/learning-futures/jamf-parent/

[4] Where guest devices accessing ATLP networks belong to staff, staff are required to adhere to the ATLP Bring your own device agreement

Devices which are used to access the internet away from the ATLP Network, including but not limited to Learning Futures iPads, are deployed using a filtering and monitoring solution. This solution will apply whenever a device connects to the internet outside of the ATLP network, for example from home internet connections or mobile hotspots.

During term time, DSLs are responsible for administering and monitoring this system and responding to alerts from the provider. Regular automated reports are provided to DSLs who must ensure that they check and investigate any alerts and take appropriate action. During holiday time, trust safeguarding leads will respond to Level 5 threat to life alerts.

The ATLP filtering and monitoring solutions will help to prevent access to inappropriate sites available on the internet. However, no automatic filtering service can be 100% effective in terms of blocking access to such sites and content. It is possible that users may accidentally access inappropriate material while using the internet. In such circumstances, users must exit the site immediately.

- Students should advise a member of staff, providing details of the site, including the web address, to reduce the possibility of the material being access again in the future. Details of the inappropriate material accessed must be logged with ATLP IT Services. The ATLP IT Services will arrange for the filtering rules to be examined to block future access to the site/content.
- Staff should contact the IT helpdesk. Staff need to be aware that if a child has told them about accessing an inappropriate site, staff should pass this onto the helpdesk using the template provided.

Action process upon receipt of a safeguarding alert

- All safeguarding alerts from Smoothwall during the working day should be actioned on the same day wherever possible.
- Level 3, 4 and 5 alerts that are received during the evening or at the weekend (before the app removal time) should be actioned on the next working day.
- Level 5 alerts that indicate a potential threat to life will require immediate action to be taken. During term time, this means that the headteacher, head of school or designated safeguarding lead will receive a phone call to alert them that a student may be at risk of serious harm. They should contact the student's parents without delay. If they are unable to contact the student's parents, they should contact the police. They should try to contact a colleague to let them know that they are doing this, seek support for their decision and discuss their own well-being. They should, as soon as possible, record the actions they have taken in response to the concern. DSLs who have had to respond to a Level 5 threat to life alert should access supervision at the earliest opportunity.
- During the holidays, alternative arrangements will be in place to ensure that Level 5 threat to life alerts can be actioned.

7 Remote education

When learning cannot take place face to face (for example, in the event of school closure due to poor weather), ATLP schools may make use of remote learning. This may include the use of platforms such as Showbie or Microsoft Teams.

The delivery of learning or other forms of interaction via Teams, or any other videoconferencing facility, should be viewed in the same way as face-to-face learning. The same standards of conduct are required as would be expected in person. Staff should set clear expectations for students' behaviour expected during online remote learning. Any incidents of poor behaviour will be dealt with in line with the school's behaviour policy.

Leaders must ensure that all staff leading online learning sessions have been appropriately trained in the appropriate use of the technology and the controls to effectively safeguard participants from in appropriate activity.

The use of such technology may include the use of cameras. If staff are to use cameras to deliver online remote learning, this must be discussed and agreed with school leaders.
Parents and carers will be aware of what their children are being asked to do, including sites they will be asked to use and school staff their child will interact with.

8 Communication with parents and carers

Parents and carers play a crucial role in ensuring that their children are kept safe online. We recognise that for many parents, keeping up to date with online safety risks can be challenging. We are therefore committed to helping parents and carers understand the issues related to online safety. This includes but is not limited to:

- Workshops and information sessions
- Newsletters
- Messaging services.

Annexe A Useful links and resources

Department for Education

Keeping children safe in education 2023 (publishing.service.gov.uk)
Meeting digital and technology standards in schools and colleges - Guidance - GOV.UK (www.gov.uk)
Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)
Meeting digital and technology standards in schools and colleges - Broadband internet standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)
Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)
Data protection in schools - Data protection policies and procedures - Guidance - GOV.UK (www.gov.uk)
Harmful online challenges and online hoaxes - GOV.UK (www.gov.uk)

Home Office

The Prevent duty: safeguarding learners vulnerable to radicalisation - GOV.UK (www.gov.uk)

Information Commissioner's Office

Data Protection Impact Assessments (DPIAs) | ICO

London Grid for Learning (LGfL)

Broadband and Beyond - Online Safety Audit (lgfl.net)

Southwest Grid for Learning (SWGfL)

360 Degree Safe - Online Safety Review Tool | SWGfL

National Cyber Security Centre

Cyber security training for school staff - NCSC.GOV.UK

UK Safer Internet Centre

2023 Appropriate filtering and monitoring definitions published - UK Safer Internet Centre
Check Your Internet Connection Blocks Child Abuse & Terrorist Content (swgfl.org.uk)
Filtering Provider Responses - UK Safer Internet Centre
Appropriate Filtering and Monitoring - UK Safer Internet Centre
Establishing appropriate levels of filtering (UKSIC)
Online safety in schools and colleges: questions from the governing board - GOV.UK (www.gov.uk)

Digital Resilience

Digital Resilience : Headstart Kernow

Remote Education

Safeguarding and remote education - GOV.UK (www.gov.uk)

Providing remote education: guidance for schools - GOV.UK (www.gov.uk)

Undertaking remote teaching safely | NSPCC Learning

Annexe B Annual Review

The ATLP intends to adopt the UK Safer Internet Centre ‘Filtering and Monitoring Checklist Register’ until further notice. This will be subject to regular review and any such changes will be updated in this Annexe.

filtering-and-monitoring-checklist.docx

Annexe C Categories of concern

All alerts received from Smoothwall are categorised and given a level of risk. These are both decided upon by the Smoothwall operator analysing the activity on the device.

The levels of risk are given in the table below

Categories of concern	Level	Reason
• Offensive user • Sexual Content • Vulnerable person • Bullying violence • Over sharer • Grooming • Terrorism/Extremism	1	Content which poses no risk on its own but is logged in case it becomes relevant in the future.
	2	Low level risks that will largely be ignored unless they escalate into a higher-level risk in this or other risk categories.
	3	Mild risks that may escalate into more serious risks.
	4	Moderate general risks that may require attention within the next few days.
	5	Serious general risks that require immediate attention.

Profile	Description
Offensive User	Communicates with: • Profanity (without bullying or threats) • Distressing and objectionable subjects or images
Sexual Content	Frequent sharing of: • Sex talk, sexual overtures or innuendos • Explicit images, video or text
Vulnerable Person	Expresses: • Credible threats of suicide, suicidal ideation, or self-harm • A current risk of sexual or physical abuse offline • Suffering from an untreated eating disorder • Severely distressed or traumatised
Bullying/Violence	Uses online content to: • Intimidate, threaten or harass others online • Encourage others to exclude individuals • Shame, humiliate or embarrass an individual by posting visual or text content • Repeatedly engage in the public abuse or malicious criticism of others
Oversharer	Exposes data about themselves or another person: • Personally identifiable information • Contact details or location • Login or financial information
Grooming	• Interacts as a suspected person 18 or older to: Desensitise and normalise a minor to sexual discussion or imagery • Establish trust with a minor by offering sympathy Encourage a minor to share contact or identity information • Request images or video from a minor • Attempt an offline meeting with a minor
Terrorism/Extremism	Threatens to:

	• Harm, kidnap or execute a person • Participate in acts of terrorism including biological attacks, bombing, vandalism or arson • Promotes violence, intimidation or terrorist activities with: • Political, ideological or religious propaganda • Rationalisation or moral duty • Targeting and demonising groups by their perceived identities
General Risk	Contains concerning or unusual activity that does not fit the predefined risk categories but should be reviewed by your school.