LYMM HIGH SCHOOL

Online Safety Policy

Date created:	April 2018
Date review due:	October 2026
Next review due:	October 2028
Version:	5
Policy owner:	DPO / DSL / ICT Manager
Ratified at Staff & Student Wellbeing Committee:	October 2026

Contents

1. Aims 3
2. Legislation and guidance 4
3. Roles and responsibilities 4
4. Educating pupils about online safety 6
5. Educating parents about online safety 7
6. Cyber-bullying 7
7. Acceptable use of the internet in school 8
8. Pupils using mobile devices in school 9
9. Staff using work devices outside school 9
10. How the school will respond to issues of misuse 9
11. Training 9
12. Filtering, monitoring and cyber security 10
13. Monitoring arrangements 11
14. Links with other policies 11
Appendix 1: Staff Acceptable Use Policy (AUP) 12
Appendix 2: Lymm High School Acceptable Use Policy (AUP) for Students 14
Appendix 3: Acceptable Use Policy (AUP) for Wi-Fi on Personal Devices 15
Appendix 4: online safety training needs – self-audit for staff 16
Appendix 5: online safety incident report log 17

Online safety policy (E-Safety)

Lymm High School recognises that ICT and the Internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the Internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good online safety. It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online.

Online safety covers the Internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of online safety falls under this duty. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. Online safety is a whole-school issue and responsibility. Online safety also covers newer technologies such as generative artificial intelligence (AI), which can be used to create convincing fake or explicit images and videos (sometimes called "deepfakes"), and AI chatbots that simulate human conversation.

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures, which are outlined in our **Behaviour Policy.**

1. Aims

Our school aims to:

Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors

Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology

Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Our approach to online safety addresses four areas of risk (the "4Cs" set out in Keeping Children Safe in Education):

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, radicalisation and extremism, and misinformation, disinformation and conspiracy theories

Contact – being subjected to harmful online interaction with other users, such as peer pressure, commercial advertising and adults posing as children or young adults to groom or exploit them, and interactions with generative AI systems that simulate human conversation

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (including images created or altered using AI), sharing other explicit images, and online bullying

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education (KCSIE) 2026, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It also takes account of the DfE's statutory guidance on mobile phones in schools, the DfE's filtering and monitoring standards and cyber security standards for schools and colleges, the DfE's guidance on generative AI in education (including its product safety standards for generative AI), and the UK Council for Internet Safety (UKCIS) guidance Sharing nudes and semi-nudes: advice for education settings working with children and young people.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. It also takes into account the Online Safety Act 2023, the Children's Wellbeing and Schools Act 2026, the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The policy also takes into account the National Curriculum computing programmes of study. This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board will make sure that appropriate filtering and monitoring systems are in place, that their effectiveness is reviewed at least once every academic year, and that a record of these reviews and checks is kept (see section 12). The governing board will also make sure that the school has regard to the DfE's cyber security standards for schools and colleges.

The governors who oversee online safety are the Safeguarding Governors.

All governors will:

Ensure that they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 1)

3.2 The headteacher

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

The headteacher will make sure that a named member of the senior leadership team (SLT), currently Ruth Ball, is responsible for filtering and monitoring, and that the school's mobile phone arrangements follow the DfE's statutory guidance on mobile phones in schools.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputy DSLs are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, 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 and other staff, as necessary, to address any online safety issues or incidents

Understanding the school's filtering and monitoring systems and processes, acting on safeguarding concerns raised by monitoring, and supporting the SLT lead with the annual review of filtering and monitoring

Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)

Liaising with other agencies and/or external services if necessary

Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.

Carrying out regular checks of filtering and monitoring across school devices, networks and locations, keeping a record of these checks, and supporting the SLT lead and DSL with the annual review

Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

Maintaining the school's cyber security controls, including multi-factor authentication (MFA) on all staff and pupil accounts, encryption of school laptops, regular software updates and backups, in line with the DfE's cyber security standards and the school's Cyber Essentials certification

Conducting a full security check and monitoring the school's ICT systems on a regular basis

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

Reporting any safeguarding concerns identified through filtering and monitoring to the DSL promptly

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

Maintaining an understanding of this policy

Implementing this policy consistently

Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 1), and ensuring that pupils follow the school's terms on acceptable use (appendix 2)

Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

Reporting to the DSL any concerns about filtering and monitoring, for example if they witness or suspect unsuitable material has been accessed, if they are able to access content that should be blocked, or if filtering is stopping legitimate teaching and learning

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

Notify a member of staff or the headteacher of any concerns or queries regarding this policy

Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

Parents and carers, UK Safer Internet Centre: https://saferinternet.org.uk/guide-and-resource/parents-and-carers

Parents and carers, Childnet International: https://www.childnet.com/parents-and-carers/

Parent factsheet, Childnet International: Parents and Carers resource sheet | Childnet

Parental controls and advice, Internet Matters: https://www.internetmatters.org/

Thinkuknow (National Crime Agency CEOP Education): https://www.thinkuknow.co.uk/parents/

3.7 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 (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. This includes Computing and statutory Relationships, Sex and Health Education (RSHE).

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 safe use of social media and the internet will also be covered in other subjects where relevant.

Pupils will also be taught about emerging risks, including misinformation and disinformation, the risks of sharing nudes and semi-nudes (including images that have been digitally altered or generated using AI), online scams and sextortion, and how to use generative AI tools safely and responsibly, including understanding their limitations.

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.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

The school will talk to parents about the online systems their child is asked to use in school and who their child will be interacting with online, and will reinforce the importance of children being safe online when away from school. Parents will be informed in advance of changes that affect their child's school account, such as two-step verification on pupils' Microsoft accounts.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 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 repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school's website also displays information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Incidents involving nudes or semi-nudes, including images that have been digitally altered or generated using AI ("deepfakes"), will be referred to the DSL and managed in line with the UKCIS guidance Sharing nudes and semi-nudes and our child protection and safeguarding policy.

6.3 Examining electronic devices

The headteacher, and staff authorised by the headteacher, have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices (phone, tablet, laptop etc) where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

Cause harm, and/or

Disrupt teaching, and/or

Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

Delete that material, or

Retain it as evidence (of a criminal offence or a breach of school discipline), and/or

Report it to the police

Staff must not view, copy, print, share, store or save any image, video or file that they suspect may be a nude or semi-nude image of a child, and must not delete it themselves. Instead, they should confiscate the device, avoid looking at the material and report it to the DSL immediately, who will decide on next steps in line with the UKCIS guidance.

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All users logging in to the school network are expected to digitally sign an agreement regarding the acceptable use of the ICT systems and Internet (appendices 1, 2 and 3).

Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. This includes the use of school accounts and devices, and of any generative AI tools provided by the school.

Staff and pupils should only use generative AI tools that have been approved by the school, and must not enter personal or sensitive information about pupils, staff or others into AI tools that have not been approved. Pupils must follow the JCQ rules on the use of AI in assessments.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils' mobile phones are secured in a locked magnetic pouch at the start of each school day and unlocked at the end of the day, so pupils do not have access to them during lessons, the time between lessons, break times or lunchtime. This is in line with the DfE's statutory guidance on mobile phones in schools. Further detail is set out in the school's behaviour policy.

Any exceptions (for example, where a pupil needs a device to manage a medical condition) must be agreed in advance by the school.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which will result in the confiscation of their device and a 40 minute lunch time detention.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 1.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. School data must not be stored on removable media such as USB drives, and should be accessed through school-controlled cloud services (for example, Microsoft 365 and OneDrive).

Staff accounts are protected by multi-factor authentication (MFA). Staff must never approve a sign-in prompt they did not start, and must report any unexpected prompts or suspicious emails to the ICT team straight away. School laptops are encrypted and managed centrally, and must be connected regularly so that they receive security updates. Staff who access school systems on a personal device must keep that device secure (for example, with a screen lock and up-to-date software) and must not store school data on it.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). Training will include the school's filtering and monitoring arrangements, staff roles and responsibilities in relation to them and how to escalate concerns, as well as emerging risks such as generative AI, deepfakes and sextortion.

The DSL and deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Filtering, monitoring and cyber security

To further support schools and colleges in England to meet digital and technology standards, the Department for Education published Filtering and Monitoring Standards in March 2023. These standards have since been updated, most recently to address the risks of generative AI, and KCSIE 2026 requires schools to review the effectiveness of their filtering and monitoring at least once every academic year.

Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

Lymm High School uses a combination of systems to keep users safe online. On the school network, our Sophos XGS firewall filters content based on age-appropriate categories, blocking harmful or inappropriate material and providing detailed activity reports. School-managed devices that are taken off site, such as the Chromebooks assigned to pupils, have Smoothwall Filter installed, so they remain filtered when used at home. Smoothwall Monitor covers all staff and pupils, and sends real-time alerts about concerning activity to the safeguarding team so that concerns can be identified and acted on quickly.

Filtering applies to all devices connected to the school network, including personal devices on the school Wi-Fi. Staff and pupils who connect a personal device sign in with their own school username and password, so their internet use is filtered by the same age-appropriate rules as on school computers and is logged against their account. Guest Wi-Fi is kept separate from the school network and is filtered by the school's default rules.

The effectiveness of filtering and monitoring is reviewed at least once every academic year by the member of the senior leadership team responsible for filtering and monitoring (currently Ruth Ball), supported by the DSL and the ICT Manager. The review includes testing filtering on different devices and in different locations across the school, and a record is kept of the checks carried out, any issues found and the action taken. An additional review will take place whenever there is a significant change, such as a new system, a new safeguarding risk or a change in how pupils access the internet.

Generative AI tools are subject to the same filtering and monitoring expectations. Before approving an AI tool for pupil use, the school will consider the DfE's product safety standards for generative AI and whether its filtering and monitoring can identify risks arising from pupils' use of the tool, such as interactions with AI chatbots.

Cyber security

Protecting personal information and keeping the school's systems secure is part of safeguarding. The school has regard to the DfE's cyber security standards for schools and colleges and holds Cyber Essentials certification. Controls include multi-factor authentication on all staff and pupil accounts, a managed firewall, protection against viruses and malware, encryption of school laptops, regular software updates, backups and independent security audits.

Additional guidance

UK Safer Internet Centre

Appropriate filtering and monitoring - UK Safer Internet Centre

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every 2 years by the DPO, DSL and ICT Manager. At every review, the policy will be shared with the Staff & Student Wellbeing Committee. The policy will be updated sooner if statutory guidance changes. Filtering and monitoring arrangements are reviewed every academic year, separately from this policy (see section 12).

14. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Staff code of conduct
- Data protection policy and privacy notices
- Complaints procedure
- Mobile phone arrangements (set out in the behaviour policy)

Appendix 1: Staff Acceptable Use Policy (AUP)

Introduction:

Welcome to Lymm High School! As a staff member, you play a crucial role in creating a positive and secure digital learning environment. This Acceptable Use Policy (AUP) outlines the guidelines for appropriate technology use.

User Responsibilities:

- Professional Conduct: Conduct yourself professionally online, maintaining the same level of respect and courtesy as in face-to-face interactions.
- Confidentiality: Respect the confidentiality of student and staff information. Do not share sensitive information without proper authorisation.
- Technology Competence: Stay updated and familiarise yourself with the technology tools used in the school environment. Attend relevant training sessions.
- Legal Compliance: Adhere to all applicable laws and regulations governing the use of technology in an educational setting. Stay informed about relevant legislation and ensure compliance in your digital activities.

Internet Usage:

- Content Filtering: Access only school-approved websites and content. Report any inappropriate content encountered during your use of technology. Report to the DSL any concerns about content that should be blocked, or about filtering that is preventing legitimate teaching.
- Professional Communication: Use school-provided communication channels for professional purposes. Avoid engaging in personal or inappropriate online discussions.

Device Usage:

- Equipment Care: Treat school devices with care. Report any technical issues promptly, and do not attempt to modify or repair devices without authorisation.
- Software/Applications: Do not download, install, or share unauthorised software.
- Account Security: Keep your password private and use multi-factor authentication (MFA) as required. Never approve a sign-in prompt you did not start, and report unexpected prompts or suspicious emails to the ICT team straight away.
- Data Protection: Store school data only in school systems (for example, OneDrive, SharePoint or the MIS). Do not use USB drives or personal cloud storage for school data, and lock your screen when you leave a device unattended.
- Generative AI: Use only AI tools approved by the school, and never enter personal or sensitive information about pupils, staff or others into an AI tool that has not been approved.
- Pupils and Personal Devices: Do not use personal devices to photograph or record pupils, and do not contact pupils through personal accounts or social media.

Consequences of Violation:

- Consequences: Failure to comply with this AUP may result in disciplinary action, including but not limited to loss of technology privileges, professional consequences, or legal action.

- Reporting: If you witness any violation of this AUP, report it to the appropriate school authorities immediately.

Conclusion:

By logging in, you agree to abide by this Acceptable Use Policy. Lymm High School reserves the right to monitor, inspect, and disclose any information transmitted over the school's network.

Thank you for your commitment to maintaining a positive and secure digital learning environment at Lymm High School!

Appendix 2: Lymm High School Acceptable Use Policy (AUP) for Students

Introduction:

Welcome to Lymm High School! As part of our commitment to creating a safe and productive digital learning environment, we expect all students to use school-provided technology responsibly and ethically. This Acceptable Use Policy (AUP) outlines the guidelines for appropriate technology use.

User Responsibilities:

- Respect for Others: Treat everyone with kindness and respect online, just as you would in person. Avoid bullying, harassment, or any form of harmful behaviour.
- Privacy and Safety: Protect your personal information and respect the privacy of others. Do not share passwords, addresses, phone numbers, or any sensitive information or engage in online activities that could compromise your well-being or that of your peers.
- Digital Citizenship: Be a responsible digital citizen. Use online resources for educational purposes, and always consider the impact of your online actions.
- Legal Compliance: Adhere to all laws and regulations related to technology use. Be aware of the legal implications of your online activities and ensure compliance with applicable legislation.
- Account Security: Keep your password private and never use anyone else's account. Set up two-step verification on your school Microsoft account when asked, and never approve a sign-in request you did not make – tell ICT Services straight away.
- Images and Sharing: Never take, share or ask for nude or semi-nude images of anyone, including fake or AI-generated images. If someone asks you for an image or sends you one, tell a trusted adult or the DSL.

Internet Usage:

- Content Filtering: Access only school-approved websites and content. Do not attempt to bypass content filters, and report any inappropriate content you may encounter.
- Online Communication: Use school-provided communication channels for educational purposes. Avoid engaging in personal or inappropriate online discussions.
- Plagiarism: Always give credit to the original creators of content. Plagiarism is not tolerated, whether it's for assignments, projects, or any other digital work.
- Artificial Intelligence (AI): Only use AI tools the school allows, and follow your teachers' instructions on when AI may be used. Never present AI-generated work as your own, and never use AI to create images or content of other people without their permission.

Device Usage:

- Equipment Care: Treat school devices with care. Report any technical issues promptly, and do not attempt to modify or repair devices without authorisation.
- Software/Applications: Do not download, install, or share unauthorised software.

Consequences of Violation:

- **Consequences:** Failure to comply with this AUP may result in disciplinary action, including but not limited to loss of technology privileges, detention, or suspension. Serious violations may involve law enforcement.
- **Reporting:** If you witness any violation of this AUP, report it to a teacher or school staff member immediately.

Conclusion:

By logging in, you agree to abide by this Acceptable Use Policy. Lymm High School reserves the right to monitor, inspect, and disclose any information transmitted over the school's network.

Thank you for helping us maintain a positive and secure digital learning environment!

Appendix 3: Acceptable Use Policy (AUP) for Wi-Fi on Personal Devices

Access to the Lymm High School network is restricted to authorised users and requires acceptance of the Terms & Conditions below.

Staff and pupils connect personal devices by signing in with their own school username and password; internet use is filtered and logged against that account. Guests are given separate access, which is filtered and kept apart from the school network.

By connecting a device to the school Wi-Fi, you agree to this policy. This may be presented as evidence should any of the acceptable use guidelines be contravened.

You are responsible for ensuring that it has been fully read and understood.

- Users will only access school systems using their own username and password, which will not be shared. Nor will users allow their files to be accessed or access files belonging to another user.
- Users are responsible for any personal removable media (such as USB drives) and all contents contained therein.
- Users will not engage in any activity that may threaten the integrity of the school's ICT Systems, or any activity that attacks or corrupts the computer system.
- Users are responsible for all e-mails sent from their account and for all contacts made that may result in an e-mail being received.
- All email messages must be polite, responsible. Use Blind Carbon Copy (BCC) when emailing groups of people outside the school, so that their email addresses are not shared.
- Users will not download any non-work related materials onto the school network such as executables, scripts, viruses, MP3 files, video files and copyrighted materials.
- Users will not use the school Internet for personal financial gain, gambling, advertising, inciting hatred, political purposes or to access inappropriate material such as pornographic, racist or other offensive sites.
- Users will use only the Schools' corporate email system to conduct school business.
- Users will respect the copyright of material found on the Internet.
- Users will not use Internet access on school systems to access chat rooms, post anonymous messages, forward chain letters or edit images of other students/staff for posting to social networking sites etc.
- Users will report any unpleasant material or messages sent to them. These reports will be confidential and will help protect others.
- The school maintains the right to check computer files/emails and monitor Internet sites visited. Inappropriate use may result in disciplinary action.

Appendix 4: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff?	
Are you familiar with the school's acceptable use agreement for students?	
Are you familiar with the school's acceptable use agreement for Wi-Fi on personal devices (appendix 3)?	
Do you use a strong, unique password for your school account, with multi-factor authentication (MFA) set up?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Do you know how to report a concern about filtering and monitoring (for example, content that should be blocked, or blocking that stops legitimate teaching)?	
Are you aware of the online risks linked to generative AI, such as deepfakes and AI chatbots?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 5: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**