LYMM HIGH SCHOOL

Online Safety Policy

Date created:	April 2018
Date review due:	October 2022
Next review due:	October 2024
Version:	3
Policy owner:	DPO / DSL / Head of IT
Ratified at Staff & Student Wellbeing Committee:	October 2022

Contents

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 e-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.

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

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, 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 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.

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 governor who oversees online safety is the Safeguarding Governor.

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 2)

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.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) [and deputy/deputies] 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
- Ensuring that any online safety incidents are logged (see appendix 4) 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 3 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
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- 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 4) and dealt with appropriately in line with this policy
- 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 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- 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 1)

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

- What are the issues? UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: Parents and Carers resource sheet | Childnet

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 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

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.

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 or virtual learning environment (VLE). This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

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.

6.3 Examining electronic devices

School staff 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, including mobile phones, iPads and other tablet devices, 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

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 and 2).

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.

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

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but they should be switched off and stored safely and securely in their bags throughout the duration of the school day.

Mobile phones can be used in lessons if the teacher gives advanced permission and they are supporting educational outcomes.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

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 2.

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. Data relating to the school must not leave site (USB drives etc) and should be accessed via remote desktop or school controlled cloud services (Office 365/OneDrive for example).

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).

The DSL [and deputy/deputies] 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. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

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 governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: acceptable use agreement (Staff)

Network Acceptable Use Policy

By clicking agree, you are creating a digital signature as evidence that you have read and understood the following 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.

1. 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.

2. Users are responsible for any personal removable media (USB Drives, CDs etc) and all contents contained therein.

3. 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.

4. 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.

5. All email messages must be polite, responsible and not make use of Blind Carbon Copy (BCC).

6. 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.

7. 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.

8. Users will use only the Schools' corporate email system to conduct school business.

9. Users will respect the copyright of material found on the Internet.

10. 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.

11. Users will report any unpleasant material or messages sent to them. These reports will be confidential and will help protect others.

12. The school maintains the right to check computer files/emails and monitor Internet sites visited. Inappropriate use may result in disciplinary action.

13. Staff must not engage with pupils through social networking sites and be mindful that all postings on social network sites are widely accessible.

14. Staff will not give out personal details, home addresses or telephone numbers etc

15. Staff will be ultimately responsible for ALL files and images saved on their network home drive/and on their Laptops/PC's, regardless of whether they saved it or not. Failure to comply may lead to disciplinary action regarding access to inappropriate material. This could ultimately lead to a formal warning or termination of employment contract depending on the severity.

16. Staff will keep safe any ICT equipment in their care such as Laptops, PC's, projectors, storage devices such as USB pen drives etc. Serious misuse of laptops will be treated as a disciplinary offence and may result in dismissal. Loss, damage or theft of a laptop through misuse or negligence may result in financial sanctions.

17. Staff will report any loss/theft of computer equipment or storage devices in their personal possession immediately to the Police, obtain a CRN (Crime Ref Number) and pass this on to the IT Services department and be cooperative in any requests that may follow to ascertain the nature of the loss.

18. It is the responsibility of all staff to ensure that pupils do not have access to confidential data, e.g. SIMS and must therefore be vigilant in their security measures e.g. locking out the computer if they are the primary user or logging off if it is a shared computer when leaving the room for a short period of time.

19. Staff will comply with the requirements of the Data Protection Act and the Computer Misuse Act.

20. Staff will ensure all data, in particular private and confidential data, is stored on the school network and accessed via secure remote access.

21. Staff will not transfer private, personally identifiable, or confidential school data onto portable electronic devices e.g. laptops, USB storage.

22. The transmission of school sensitive data over the internet is strictly prohibited.

23. The ordering /purchasing of goods over the internet is subject to the same authorisation procedures and limits as purchases made by other means and failure to follow the correct procedure may result in disciplinary action.

Appendix 2: acceptable use agreement (All Other Users)

Network Acceptable Use Policy

By clicking agree, you are creating a digital signature as evidence that you have read and understood the following 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.

1. 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.

2. Users are responsible for any personal removable media (USB Drives, CDs etc) and all contents contained therein.

3. 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.

4. 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.

5. All email messages must be polite, responsible and not make use of Blind Carbon Copy (BCC).

6. 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.

7. 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.

8. Users will use only the Schools' corporate email system to conduct school business.

9. Users will respect the copyright of material found on the Internet.

10. 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.

11. Users will report any unpleasant material or messages sent to them. These reports will be confidential and will help protect others.

12. The school maintains the right to check computer files/emails and monitor Internet sites visited. Inappropriate use may result in disciplinary action.

Appendix 3: 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, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: 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**