Online Safety Policy

Governors' Committee Responsible	Headteacher
Reviewer	**ICT Lead O.Chondrogianni**
Status	**Non Statutory**
Review Cycle	**3 Years**
Date Written Last Review	**March 2017** **March 2022**
Date of Next Review	**March 2025**

Online safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's online safety policy will operate in conjunction with other policies including those for Behaviour for Learning, Bullying, Curriculum, PSHE/RSE, Data Protection and Safeguarding.

Good Habits

Online safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the London Grid for Learning including the effective management of content filtering.

- National Education Network standards and specifications.

Contents

Contents 2

Why is Internet Use Important? 3

How does Internet Use Benefit Education? 3

How can Internet Use Enhance Learning? 3

Authorised Internet Access 4

World Wide Web 4

Email 4

Social Networking 4

Filtering 4

YouTube Policy 5

Managing Emerging Technologies 5

The Prevent Duty and Online safety 5

Published Content and the School Website 6

Publishing Pupils' Images and Work 6

Information System Security 6

Protecting Personal Data 6

Assessing Risks 7

Handling Online Safety Complaints 7

ICT Acceptable Use Policy 7

Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to enable children to become technologically equipped for the wider world, to assist in the development of critical thinking and assessing validity of information, assessing and managing risk, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority;
- access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in online activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- Pupils will regularly learn about online safety across the computing curriculum.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'ICT Acceptable Use Policy' & 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents are asked to give consent pupil access on the admissions form.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to LGfL and the Local Authority.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Pupils do not have access to a school email inbox and therefore will not be able to send or receive emails.
- Pupils will be assigned a unique email address and password, which will serve as their login details and will enable them to access educational content and services.
- Pupils must not reveal personal details of themselves or others in any online communication, or arrange to meet anyone without specific permission.
- Whole class communication should happen through Google Classroom or ParentPay.
- Access in school to external personal email accounts may be blocked.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Social Networking

- Access to social networking sites and newsgroups is blocked by our internet filters.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Filtering

The school will work in partnership with the Local Authority and the Internet Service Provider (LGfL) to ensure filtering systems are as effective as possible.

YouTube Policy

Videos on the file-sharing website YouTube can be used to effectively support many areas of the curriculum. The popular site contains a selection of videos which cover the range of topics focused on at Lime Tree Primary School. Additionally, there is a variety of music, song and dance performances appropriate for children. When these videos are used safely and appropriately, they can be an extremely beneficial resource for Class Teachers and Support Staff.

However, there are potential risks when working with YouTube that staff should be aware of. For example, despite a filter/flagging policy being in use on YouTube, inappropriate images, pop-up advertising, unsuitable written comments, or bad language can still all be accidentally revealed to the children. In order to prevent this from happening, the following precautions should be taken:

Finding suitable videos:

- Searches, or first observations of a potential video, should not be carried out with any child in the classroom but seen by the adult who will be responsible for sharing it with the children.
- Before showing a video to the class, the video should be watched and listened to carefully in its entirety by the Class Teacher or TA, who should look out for inappropriate content material along with any inappropriate comments that appear underneath the video.
- It is the class teacher's responsibility to make the final approval of a video.

Uploading content:

- Children should be reminded that they should not be uploading personal or school videos to public websites, such as YouTube.
- Children and parents should be reminded that there is an age limit for the use of most video services under their respective Terms of Service Agreement. The age for YouTube is 13 years old, or younger if allowed by a parent or legal guardian.
- Staff should make every effort to access video content through copyrighted and legal sources, such as subscription-based streaming services, purchased DVDs, etc. Content acquired through illegal downloading or DVD ripping should not, at any time, be allowed within the school systems and networks.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Staff should not use mobile phones to take pictures or videos of children. Staff should only use digital cameras which have been provided by the school. Mobile phones are not permitted for use anywhere in school, around the children. This applies to members of staff and other visitors to the school. Mobile phones may only be used in office areas, staffroom etc.
- The only exception to this is staff taking a mobile phone with them on a school trip/visit outside of school, for use in emergencies only.
- Children who bring mobile phones to school are required to hand them in to the school office staff every morning (or the mobile phone box managed by the class teacher) and devices are collected at home time.

The Prevent Duty and Online safety

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. We have an important role to play in equipping children to stay safe online. Internet safety is integral to our computing curriculum. Our staff are aware of the risks posed by online activity of extremists and have a duty to take action if they believe the wellbeing of any pupil is being compromised.

Published Content and the School Website

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained at the point of admission, to allow the publication of photographs on the school website.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Protecting Personal Data

Lime Tree Primary School holds the legal right to collect and use personal data relating to pupils and their families, and we may also receive information regarding them from their previous school, LA and/or the DfE. We collect and use personal data in order to meet legal requirements and legitimate interests set out in the GDPR and UK law, including those in relation to the following:

- Article 6 and Article 9 of the GDPR
- Education Act 1996
- Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013

Personal data relating to pupils at Lime Tree Primary School and their families is stored in line with the school's GDPR Data Protection Policy.

In accordance with the GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.

Handling Online Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

ICT Acceptable Use Policy

Pupils

- Pupils will be informed that Internet use will be monitored.

Staff

- All staff are required to read the Online Safety policy and ICT Acceptable Use and Agreement policy, understand their importance and have signed the ICT Acceptable Use Agreement.
- All staff will be trained in safeguarding procedures, including elements of online safety and The Prevent Duty.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to the school Online Safety policy in newsletters and on the school website. The school will also organise online safety workshops to support parents' understanding of how to best safeguard their children against potential online dangers.

Sanctions

Students / Pupils								
Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X					
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X			X			
Unauthorised use of social media / messaging apps / personal email					X		X	

Unauthorised downloading or uploading of files	X			X				
Allowing others to access school network by sharing username and passwords	X						X	
Attempting to access or accessing the school network, using another student's / pupil's account	X						X	
Attempting to access or accessing the school network, using the account of a member of staff		X			X			X
Corrupting or destroying the data of other users				X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X			X
Continued infringements of the above, following		X		X				X

previous warnings or sanctions								
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X		X				X
Using proxy sites or other means to subvert the school's filtering system					X		X	
Accidentally accessing offensive material or imagery and failing to report the incident		X	X	X	X		X	X
Deliberately accessing or trying to access offensive material or imagery		X	X	X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the		X						X

Data Protection Act								

Staff	**Actions / Sanctions**							
Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X		X				X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X				X	X		

Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X				X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules		X			X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X			X	X

Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	X					X
Actions which could compromise the staff member's professional standing		X	X					X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X					X	
Using proxy sites or other means to subvert the school's filtering system	X					X	X	
Accidentally accessing offensive material or imagery and failing to report the incident		X	X					

Deliberately accessing or trying to access offensive material or imagery				X			X	
Breaching copyright or licensing regulations		X						X
Continued infringements of the above, following previous warnings or sanctions		X					X	X