Lowerhouse Junior School, Burnley

ACCEPTABLE USE POLICY	
Written By	G.Lloyd/Headteacher
Date	September 2024
Date of Review	September 2026

Inspiring a lifelong love for learning

Aspiration

Integrity

Respect

Resilience

Introduction

The purpose of this online safety policy is to:

- establish rules, for children and staff, for using the Internet and electronic equipment in school
- describe how these fit into the wider context of our behaviour for learning.
- demonstrate the methods used to protect the children from unsuitable material

The responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians. At Lowerhouse Junior School we believe that the most effective ways of ensuring responsible internet use by our children involves a combination of site-filtering within school, of supervision and by developing a responsible attitude in our pupils in partnership with parents.

Why the Internet and emergent technology are important

Lowerhouse Junior School has a duty to provide pupils with internet access to raise educational standards, to support and promote academic achievement and to enhance the school's management information and business administration systems. Internet use is a part of the statutory curriculum and an essential tool for pupils and staff. Internet access is an entitlement for students who show a responsible and mature approach to its use. The Internet is an essential element in 21st Century life for education, business and social interaction.

How the Internet will enhance teaching and learning

Internet access at school is designed for pupil use and will include filtering of website content appropriate for pupils. Students will be taught what is acceptable and what is not acceptable and given clear instructions for safe internet use. Internet access is planned to enhance and extend learning. Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils will be taught the effective use of the Internet in research, including the skills of knowledge location and retrieval.

Managing e-mail

Pupils will have access to email accounts for use in curriculum work when needed. Pupils are to follow the school code when using their email accounts and must be polite and courteous to each other at all times. The schools behaviour and online safety policies will be followed in any instance of pupils not adhering to this. Pupils must immediately tell a teacher if they receive an offensive e-mail. Pupils are taught never to reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication. In line with the computing scheme of work followed in school, children will use Kidscapism as their main form of email communication with each other.

In our school the following statements reflect staff practice in the use of email.

• All staff users have access to the Lancashire Grid for Learning service as the preferred school e-mail system.

• Only official email addresses should be used to contact staff. There is to be no emailed contact with families and children other than through the school office email.

• The BT Lightspeed filtering service used by school should reduce the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to the BT Lightspeed service.

• All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.

• All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.

• All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.

• All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature to a member of the senior leadership team.

AI Specific Guidelines

- Transparency: When using AI tools for assessment or feedback, ensure transparency with children and parents about how the AI is being used and its limitations.
- Bias Awareness: Be aware of potential biases in AI algorithms and take steps to mitigate them.
- Data Privacy: Ensure that any data used by AI tools is handled in accordance with GDPR and other data protection regulations.
- Academic Integrity: Children must understand that using AI to generate work and submitting it as their own is plagiarism. Proper citation and acknowledgement of AI assistance is required.
- Critical Evaluation: Encourage children to critically evaluate the information provided by AI tools and to verify its accuracy.
- Appropriate Use: AI tools should be used to support learning, not to replace it. Teachers should carefully consider the appropriateness of AI tools for different tasks and age groups.

Social Networking

Social Network sites allow users to be part of a virtual community. Current popular examples of these are Facebook, Twitter, Instagram and Snapchat. These sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a Social Network site, you may have access to view other users' content, send messages and leave comments. NB: Many Social Network sites have age restrictions for membership e.g. Facebook minimum age is 13 years old. The use of social networking sites is forbidden using the schools internet for pupils and staff.

Pupil Education

Within school, pupils are educated on the use of social media through computing lessons, lessons; the curriculum used in school addresses important online safety issues such as digital footprint, what constitutes acceptable behaviour online, risks of opening links and attachments from unknown sources, and of communicating personal information through the use of email, social media or video link.

Weekly PSHE lessons, whole school assemblies and theme days such a Safer Internet Day are used in school to educate children on key issues surrounding online safety such as cyber bullying, inappropriate content, online grooming, radicalisation and online reputation.

All staff must to be aware of the following points

• They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.

• Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.

• If a social network site is used, details must not be shared with pupils and privacy settings be set at maximum.

• Pupils must not be added as 'friends' on any Social Network site. It is also advised that parents are not added as friends on these sites.

• Remember; whatever means of communication you use you should always conduct yourself in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever.

Mobile telephone

- Pupils are not allowed to use mobile phones in school.
- Staff phones must be put away during teaching sessions.
- Visitors must not use their mobile phones on school premises.
- Personal mobile phones may be used on school visits for **contacting school only** but personal phone numbers must not be used on any documents which parents or pupils may have access to and must not be used for taking photographs of pupils.

Instant Messaging

Instant Messaging, e.g. Facebook messenger and Skype, are all a popular communication tool with both adults and children. It provides an opportunity to communicate in 'real time' using text, sound and video. The BT Lightspeed filtering service blocks these sites on school by default, but access permissions can be changed at the request of the Headteacher if deemed necessary. The school's filtering service is checked regularly for its effectiveness by the Headteacher and IT Technician.

Websites and other online publications

• The point of contact on the school website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.

• Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site.

• Web site photographs will only include images of children where the school has written permission from parents.

• Pupils' full names will be used on the school website, with parental consent, when linking with learning displayed on class pages and when celebrating successes such as the weekly golden book and assembly badge winners.

• The Headteacher and school business manager will take overall editorial responsibility and ensure that content is accurate and appropriate.

• The school web site should comply with the school's guidelines for publications.

• The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

• Downloadable materials must be in a read-only format (e.g. PDF) where necessary, to prevent content being manipulated and potentially re distributed without the school's consent.

Video conferencing

Although video conferencing is not widely used in school, Lowerhouse accepts that guidelines must be in place in instance that it is used to enhance pupils learning.

• A permissions letter must be made available for parents/carers to sign giving permission for their child/children to participate in video and photographs. Children will not be appearing 'live' on the Internet through a video conferencing link.

• However, it is still important to remember that the images which are broadcast from school could be captured as a snapshot or video clip from a system receiving the broadcast.

• Approval by the Headteacher/Deputy Headteacher must be obtained in advance of the video conference taking place. All sessions should be logged including the date, time and the name of the external organisation/ person(s) taking part.

• Pupils using video conferencing equipment should be supervised at all times.

• All staff supervising video conferencing equipment should know the procedures to follow if they are unhappy with the content of a VC session e.g. how to stop or hang up the call.

• Copyright, privacy and Intellectual Property Rights (IPR) legislation will be breached if images, video or sound are recorded without permission.

Internet access and risk assessment

At Lowerhouse Junior School, children will carry out focussed searches using the Internet and any work done on the internet should be done in the presence of an adult. In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Lancashire Education Authority can accept liability for the material accessed, or any consequences of Internet access. Methods to identify, assess and minimise risks will be reviewed regularly. The Headteacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

The following outlines some of the potential risks associated with Internet use:

Commerce Pupils should be taught to identify potential risks when using commercial sites.	Advertising Privacy of information (phishing, identity fraud) Invasive software (e.g. virus, trojan, spyware) Online gambling Premium rate sites
Content Pupils should be taught that not all content is appropriate or from a reliable source.	Illegal materials Inaccurate / bias materials Inappropriate materials Copyright and plagiarism User generated content (e.g. YouTube)
Contact Pupils should be taught that contact may be made using digital technologies and that appropriate	Grooming Cyberbullying Contact inappropriate emails / blogs / instant messaging Encouraging inappropriate contact

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP and Internet Watch Foundation (IWF). Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Always report potential illegal content to the Internet Watch Foundation. (http://www.iwf.org.uk). They are licensed to investigate – **schools are not.**

Examples of illegal offences are

• Accessing child sexual abuse images
• Accessing non-photographic child sexual abuse images
• Accessing criminally obscene adult content
• Incitement to racial hatred

More details regarding these categories can be found on the IWF website - http://www.iwf.org.uk

Incident	Response
Accidental access to inappropriate material.	Minimise the webpage/turn off the monitor. Tell a trusted adult. Enter the details in the incident log book and report to LGFL filtering services if necessary. Persistent 'accidental' offenders may require further disciplinary action in accordance to the school's behaviour policy.
Using other people's logins and passwords maliciously. Deliberately searching for inappropriate material. Bringing in inappropriate electronic materials from home. Using email, chats and forums in an inappropriate way.	Inform a member of SLT – report incident to DSL if necessary. Enter the details in the incident log. Raise additional awareness of e-safety with the child/class. More serious incidents may result in further disciplinary action in accordance with the behaviour management policy.

	Consider parent/carer involvement.

Staff use of the Internet

All adults who use the school internet system must sign to accept the terms of the 'Acceptable Use' policy before using the internet in school. All adults, including teachers, supply staff, classroom assistants and any other adults who may use the internet in school, will be provided with the School Internet Policy before accessing the school's internet. Staff will be made aware that internet traffic can be monitored and traced **if** there are any concerns about inappropriate use of the internet. If any concerns are raised regarding use of the internet, or the accessing of suspected illegal material, these must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF).

Staff must never personally investigate, interfere with or share evidence as this may lead to them to committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Always report potential illegal content to the Internet Watch Foundation (http://www.iwf.org.uk). They are licensed to investigate – **schools are not.**

Social networking by staff

Social networking is an accepted and increasingly popular way of communicating. When using social network sites, such as Facebook, Instagram or Twitter, members of staff need to be aware of the following good practice:

- Social network accounts which may show personal content that could be considered to be unprofessional.
- Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- Pupils should not be added as 'friends' on staff Facebook accounts and should not be able to access the content of other social network accounts belonging to staff. It is also strongly advised that parents are not added as 'friends' on any of the social networking sites.

Staff must understand that whatever means of communication is used; they should **always** conduct themselves in a professional manner.

Staff email accounts

All members of staff at Lowerhouse are issued with an LCC email address which is the schools chosen email provider. Staff must ensure that they do not use this email address for personal use in school and must also not use a personal email address for work related emails. All staff must remember that they need to conduct themselves professionally at all times when using their school email address, if any concerns arise then these must be reported to the head teacher.

Involving parents

Parents' attention will be drawn to the School Internet Policy on the school website. Any internet issues will be handled sensitively to inform parents without causing any undue alarm. A partnership approach with parents is encouraged. This includes demonstrations, practical sessions and suggestions for safe Internet use at home. Online safety training has been made available to parents, updates relating to online safety are provided on the school newsletter by the Headteacher.

Staff Training
All staff in school, including governors, receive annual training on safeguarding and online safety.

PREVENT

***The Counter Terrorism and Security Act 2015*, section 26th February 2015 places a legal duty by the DfE on schools to have due regard to the need to prevent people from being drawn into terrorism or be subject to radicalisation.** In line with legislation to prevent possible radicalization of individuals, the school safeguards children through adherence to the school child protection policy and allowing Internet access only under staff supervision.

This Online Safety policy has been written in accordance with Lancashire County Council and Government guidelines.

This policy was written by: Hannah Marsden
Position: Senior Leader/Back Up DSL