Lindow Community Primary School

Online Safety Policy

'Caring, Learning & Achieving Together'

Contents

Policy Overview

Purpose

Lindow Community Primary School does all it can to ensure that every child is safe. The purpose of this policy is to protect all parties: the children, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. This policy should be read in conjunction with the following policies:

- Child protection and Safeguarding policy
- Behaviour Policy
- Whistleblowing policy
- Staff code of conduct (within staff handbook)
- Behaviour & Anti-bullying policy
- Data protection policy
- Social media policy

We believe that:

Children and young people should never experience abuse of any kind.

Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

The online world provides everyone with many opportunities; however it can also present risks and challenges.

We have a duty to ensure that all members of the Lindow community are protected from potential harm online.

We have a responsibility to help keep children safe online, whether or not they are using school's network and devices.

All children have the right to equal protection from all types of harm or abuse.

Working in partnership with children, their parents, carers and other agencies is essential in promoting their welfare and in helping children to be responsible in their approach to online safety.

Rationale

- Set out the key principles expected of all members of the school community at Lindow Community Primary School with respect to the use of technology.
- Safeguard and protect the pupils and staff.
- Assist school staff working with pupils to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying.

- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

Areas of concern

In line with the statutory Keeping Children Safe in Education 2024 guidance, there are four areas of concern with regard to online safety. These are: **content, contact, conduct and commercialism**.

1. Content – students must be protected from being exposed to inappropriate content and taught how to keep themselves safe from it.
2. Contact – students must be made aware of the dangers of communicating with unknown people online. It is important for children to realise that new friends made online may not be who they say they are. Students need to be aware that sharing their personal information or images with online friends puts them at risk.
3. Conduct – students must be taught about how they conduct themselves online. Their online activities can have an impact on both themselves, and others. For example, the activities of one child do bully or abuse another child.
4. Commercialism – the methods of online companies in advertising and marketing may lure students into clicking on malicious links, or purchasing things without adults' knowledge. Students need to be aware of the risk of scams through clickbaits where their personal information and computer access can be stolen, whether this be in emails, social media, etc.

Specific areas of concern for our school community can be summarised as:

1. Lifestyle websites promoting harmful behaviours
2. Hate content
3. Online bullying in all forms
4. Social or commercial identity theft, including passwords
5. Privacy issues, including disclosure of personal information
6. Digital footprint and online reputation
7. Health and well-being (amount of time spent online, gaming, body image)
8. Online grooming
9. The risks of disinformation
10. The risks of online groups recruiting children to an ideology that radicalises or incites.
11. Monitoring Google Classroom stream for content added by students.
12. Use of mobile phones on the way to and from school, and in schools.
13. Chat groups associated by websites promoted by the school, such as the Scratch forums.
14. Awareness of the harms of excessive screen times for children.
15. The risks of recording or eavesdropping during online meetings such as teams (or other media), when discussing personal information about children.
16. The inappropriate use of AI in education
17. The use of AI chatbots offering unsafe advice

Strategies to keep children safe online

We will seek to keep children and young people safe by:

- Using a recognised and trusted filtering system that protects students and staff from accessing harmful content in school. This is installed on all school devices, such as Chromebooks and iPads.
- Supporting and encouraging our children to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
- Supporting and encouraging parents and carers to do what they can to keep their children safe online.
- Having clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child.
- Reviewing and updating the security of our information systems regularly.
- Ensuring that user names, logins, email accounts and passwords are used effectively. Each student and staff should have their own login and password and this should not be shared with other users
- Ensuring personal information about the adults and children at Lindow Community Primary School is held securely and shared only as appropriate.
- Ensuring that images of children are used only after written permission has been obtained from parents/carers, and only for the purpose for which consent has been given.
- Offering support and guidance to parents on how to keep children safe online through parental workshops.
- Information for parents to keep their children safe online will be regularly updated on the school website.
- Examining and risk assessing any social media platforms and new technologies before they are used by the school.
- Ensuring a clear, progressive online safety education programme is part of our PSHE and through the Computing curriculum via the 4 Cs cover sheet.
- Ensuring there is an educational filter on the server to block inappropriate content.
- Improve student awareness of themes through devoted assemblies and teaching resources during Online Safety week.
- Staff run an annual online safety poster competition, encouraging children to talk to parents and staff about risks online.
- Be vigilant of the dangers and impact of privacy if children having smartwatches, phones etc, that have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G), in school - without school safeguards. They could be used to record, search and share without consent.

Roles and responsibilities

Governors

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

The governing body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing body will also make sure all staff receive regular online safety updates (via email, ebulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

The governing body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discussed with IT staff and service providers, what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs. The governor who oversees online safety is Craig McGuire.

Headteacher

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

Reviewing the filtered items from the filtering and monitoring system.

Annual online self-audit tools such as: 360 safe website or LGfL online safety audit should be completed. This follows the advice of the Keeping Children Safe in Education 2024.

The headteacher, and any member of staff authorised to do so by the headteacher DSL/SLT can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

All users:

- Are responsible for using the school IT and communication systems in accordance with this policy
- Are aware that use of all school owned devices is monitored.

- Understand the significance of misuse or access to inappropriate materials and are aware of the consequences.
- Understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so.
- Understand the importance of adopting good online safety practice when using digital technologies in and out of school.
- Know and understand school policies on the use of mobile and hand-held devices including cameras.
- Know that school owned devices are the only devices permitted for use during lesson time.
- Know that the School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. This includes school-assigned and personal devices.

The Designated Safeguarding Lead for Online Safety

- Incorporating guidance set out by the government for teaching Online Safety through Assemblies, PSHE (RSE) and the computing curriculum.
- Hold several whole school assemblies on Online Safety or invite guest speakers to do so
- Each computing portfolio, from Year 2 to Year 6, will have an online cover sheet in Google Classroom where the discussions about the 4 Cs (Conduct, Contact, Content, Commercialisation) are linked to their specific computing topic, are discussed and evidenced.
- The school will provide age-appropriate books, with fairy tale characters, that will engage younger children with the themes of online safety – these will be on display in a public area when not in use.
- Display boards will be created with student work to encourage engagement of the 4 Cs of online safety.
- Organising events for the annual Internet Safety Day
- Disseminate training for online safety with staff
- The online Safety lead will engage with resources from *Project Evolve,* and other online safety resources, to facility any training needs for the staff.
- Providing clear and specific directions to staff on how to behave online through our staff code of conduct.
- Liaising with the headteacher, who monitors the school filtering system, as to the adequacy of the system.
- Working under the leadership of the headteacher, annual online self-audit tools such as: 360 safe website or LGfL online safety audit should be completed. This follows the advice of the Keeping Children Safe in Education 2024.
- Updating the website with information for parents, signposting useful sites for parents and children.

Staff at Lindow Community Primary School:

- Know to be vigilant in the supervision of children at all times.

- Be vigilant of signs of radicalisation or extremism in computer use, in accordance with the Prevent guidance.
- Know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open internet searching is required with younger pupils.
- Staff have their own unique usernames and passwords and know they must always keep their passwords private.
- Apps such as ClassDojo should not be logged in on class iPads
- Staff know to log out or lock devices when not in use.
- Staff have their own email account that is for professional use only.
- Follow the school's social media policy, ensuring that no reference is made to the school on personal accounts.
- Know personal devices should be turned off or put on silent. These are not permitted for use in the presence of children.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- Know that in an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141 or switching off 'caller ID') their own mobile number for confidentiality purposes.
- Staff follow the school's data protection policy for use of digital photographs and videos – permission from a parent carer must be given before images of children are shared online. These can only be shared for the purpose given. Pupils must only be identified by their first name in any images shared online.
- Chat streams, such as on Google Classroom, will be monitored by class teacher for appropriate online conduct
- Mobile phones – for year 6 students only – must be given to their class teacher at the beginning of the day and kept safe by this teacher. Mobile phones that have been brought to school and not given to the teacher can be confiscated and parents contacted. This is to protect students and staff that may have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G) without school safeguards.
- The filtering system must be monitored by the designated safeguarding lead to check what content has been searched for and filtered.
- Staff will receive annual training from Online Safety lead or external provider on the current risks of the online world.
- If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:
    - Not view the image
    - Confiscate the device and report the incident to the DSL immediately

Parents/Carers:

- Should know and understand what the school's online expectations are and what sanctions result from misuse.
- Should know that only pupils in year 6 (or younger year groups with explicit agreement by the Headteacher in exceptional circumstances) are permitted to bring their own mobile phone into school and should only do this if they have permission to make their own way to

and from school. All personal pupil mobile devices are stored in the teacher's desk during the day. School will not accept responsibility for the loss, theft or damage of any mobile phone brought into school.

- Are encouraged to keep track of their child's online behaviours and alert the school if they find any evidence of concerning behaviour of students from school.
- Parents/carers are encouraged to respect the age restrictions set by social media companies, which is often a minimum of 13-years-old.
- Parents report to school any evidence of cyber-bullying.

Cyber-bullying

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 1 person or group by another person or group, where the relationship involves an imbalance of power.

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. Class teachers will discuss cyber-bullying with their year groups.

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).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour and anti-bullying 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.

Artificial Intelligence

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by staff at Lindow School. AI could have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Incident management

At Lindow Community Primary School:

All members of school staff are encouraged to be vigilant and to report any incident immediately to a member of the senior leadership team. Where the incident is a safeguarding matter, this should be reported to the Designated Safeguarding Lead.

Following an incident, the appropriate behaviour, safeguarding or anti-bullying policy will then be followed.

Support is actively sought from other agencies as needed (i.e. the local authority, SCIES, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police) in dealing with online safety issues.

Monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety within the school.

Incidents are recorded using CPOMs

Following an incident, parents/carers will be informed.

The Police will be contacted if one of our staff or pupils has conducted themselves inappropriately online, if it considered to have broken the law.

We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

If online abuse occurs, we will respond to it by:

- Following the school's safeguarding policy and procedures for responding to abuse (including online abuse).
- Informing the school's Designated Safeguarding Lead and recording all incidents.
- Providing support and training for all staff on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation.
- Making sure our response takes the needs of the person experiencing abuse, any bystanders and our school as a whole into account.
- Reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

Policy Date: March 2025

Review Date: March 2026

Ratified by Governors: April 2025