Linden Lodge School

Provider of specialist education since 1903

Title:	Online safety Policy
Type:	POLICY
Review Cycle Frequency:	1 year
Lead Staff:	Deputy Head
Support:	Designated Safeguarding Lead

VERSION CONTROL:

Version No	New document or reasons for revision	Agreed by	Date
1	Migration to new document version control system	Office	April 2021
2	Policy review	Lead staff	April 2022
3	Staff update	Lead staff	Sept 2022
4	Policy review	Lead staff	Spring 2024
5	Policy update	Lead staff	Spring 2025
6	Policy review	Lead staff	Spring 2026

LINKED INTERNAL DOCUMENTS:

Safeguarding & Child Protection policy
Staff Acceptable Use policy
Data protection policy
Social Media Policy

LINKED EXTERNAL DOCUMENTS:

Equalities Statement:

We have carefully considered and analysed the impact of these policies on equality and the possible implications for people with protected characteristics, as part of our

commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

Requests for Paper Copies:

If you require this policy in a different format e.g. print or braille please contact

Co-Headteachers@lindenlodge.org.uk

Wellbeing statement of commitment

We are committed to providing a healthy working environment and improving the quality of working lives for all staff and students. The wellbeing strategy aims to support our mission, core values and freedom of thought and expression, freedom from discrimination and the recognition that our community is our greatest asset. For further information on our school's commitment to wellbeing, please see the Mental Health and Wellbeing Policy and Strategy document, or visit our school website.

Contents

1. Aims

Linden Lodge School aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors.
- Identify and support groups of students that are potentially at greater risk of harm online than others.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes.
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), 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 (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the DfE'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 students' 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.

3. Roles and responsibilities

3.1 The governing board

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

The governing board 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 board will also make sure all staff receive regular online safety updates (via email, e-bulletins 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 board will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board will make sure that the school teaches students how to keep themselves and others safe, including online.

The governing board will make sure that 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's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the 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 the school's safeguarding needs.

All governors will:

- Make sure they have read and understand this policy.

- Agree and adhere to the terms on acceptable use policy of Linden Lodge School's online systems.
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school approach to safeguarding and related policies and/or procedures.
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted and meaningful for all students.

3.2 The Co-Headteachers

The Co-Headteachers are responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) are set out in our safeguarding policy, as well as relevant job descriptions.

The DSL takes overall responsibility for online safety, supported by the deputy head teacher, in school, in particular:

- Supporting the Co-Headteachers in making sure that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Co-Headteachers and governing board to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly.
- Working with the Director of IT to make sure the appropriate systems and processes are in place.
- Working with the Co-Headteachers, Director of IT and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school's child protection policy.
- Responding to safeguarding concerns identified by filtering and monitoring.
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately.
- Updating and delivering staff training on online safety.
- 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.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

3.4 The Director of IT and IT Team is responsible for:

Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

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

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

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 IT systems and the internet, and making sure that students follow the school's terms on acceptable use.
- Knowing that the DSL, supported by the Director of IT, is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing.
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to make sure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Co-Headteachers of any concerns or queries regarding this policy.
- Make sure that their child is supported within the acceptable use of the school's IT systems and internet.

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

- What are the issues? – UK Safer Internet Centre

- Help and advice for parents/carers – Childnet
- 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 IT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Educating students about online safety

At Linden Lodge we are fully aware that due to our students learning needs, their end points of learning within online safety will differ between curriculum pathways. Therefore, online safety will be personalised for our students across all curriculum pathways, ensuring that all students will leave Linden Lodge School having had the opportunity to develop their skills and knowledge within online safety in a way that is meaningful and appropriate to them.

Within each curriculum area, we expose our students to an accessible and personalised online safety educational offer.

Our key areas of learning within online safety across the curriculums includes but is not limited to the following:

In **EYFS+** our students have opportunities to develop skills and knowledge within:

- Using technology safely and respectfully.
- Identifying where to go for help.
- Beginning to understand and recognise acceptable and unacceptable behaviours when using technology.
- Beginning to understand that technology serves a purpose and can be used to support their access to learning.

In **Pre-Formal+** our students have opportunities to develop skills and knowledge within:

- Exploring technology to support development within cause and effect.
- Develop an understanding that technology has a purpose and can be used to make something happen.
- Develop an understanding that technology should be used in a safe and respectful way.
- Begin to indicate that they need help when using technology.

In **Semi-Formal+** our students have opportunities to develop skills and knowledge within:

- Using technology safely and respectfully.
- Identifying where to go for help.
- Begin to understand acceptable and unacceptable behaviour.

- Beginning to recognise when technology can be used to support their access to learning.
- Recognising when help is needed and indicating for help.

In **Formal+** our students have opportunities to develop skills and knowledge within:

- Using technology safely, respectfully and responsibly.
- Recognising acceptable and unacceptable behaviour.
- Knowing who to go to when they need help.
- Being independent in identifying technology that can support their access to learning and being able to implement it within lessons.
- Identifying a range of ways to report concerns about content and contact.
- Leaning how to be discerning in evaluating digital content.
- Understanding a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.
- Being able to recognise inappropriate content, contact and conduct, and know how to report concerns.
- Understanding how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns and what to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
- Understanding that there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met.
- Understanding the importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online.
- Understanding online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up.
- Understanding that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- Understanding that they should not provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Students should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Our students have access to online safety lessons that support them to understand the serious risks of sending material to others, including the law concerning the sharing of images.

- Understanding that forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Our students should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Our students are supported in their understanding of knowing how to seek support and that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Our students are taught that sharing indecent images of people over 18 without consent is a crime.
- Understanding how to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- Understand that criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion.

Sixth form+ online safety

Within sixth form our students use technology to further develop skills needed for adulthood. Our students will have an awareness of risks associated to going online and to keep safe. Our students will be able to recognise the risks linked to the use of the internet.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety within our newsletters and through in-person/ virtual training sessions.

This policy will also be shared with parents/carers.

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

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

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

6.2 Preventing and addressing cyber-bullying

At Linden Lodge School, we understand that not all of our students will understand the concept of cyber-bullying. Therefore, we personalise support for our students through our curricular.

Where appropriate, we will actively discuss cyber-bullying with our students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Our staff team 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 online safety inc. cyber-bullying, its impact and ways to support our students, as part of safeguarding training.

The school also provides training to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

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

- Poses a risk to staff or students, 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.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the Co-Headteachers.
- Explain to the student why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it.
- Seek the student's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the Co-Headteachers to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The student and/or the parent/carer refuses to delete the material themselves.

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, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

6.4 Artificial intelligence (AI)

Any use of artificial intelligence should be carried out in accordance with our AI policy.

7. Acceptable use of the internet in school

All students, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet

in accordance with our Acceptable use policy. 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 students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the Acceptable Use policy.

8. Students using mobile devices in school

We are aware that for some of our students, they have long journeys into school and back home each day and the use of mobile devices during this travel time is important for them. Therefore, students may bring mobile devices into school, but are not permitted to use them during school time. When arriving at school, mobile devices must be handed to their class teacher/ class team, where it will be stored securely until the end of the day.

Residential: mobile phone use

Linden Lodge School recognise that during our pupil's time within the residential unit they will be accessing technology including the use of mobile phones and tablets. We also recognise that these times may not always be supervised by the staff members working on the units. Therefore, we have initiated the following in order to support our pupil's safe access to the internet:

- Timed blocks on websites that can offer access to inappropriate materials
- Internet and online safety lessons based on Google's framework of Sharp, Alert, Secure, Kind, Brave, Be internet legends, on the following areas: Think before you share/ Check it's for real/ Protect your stuff/ Respect each other/ When in doubt, ask.
- Robust firewall and filtering systems in place
- Staff awareness/ supervision of pupil spaces such as lounge/ kitchens

9. Staff using work devices outside school

Staff should use school, hardware, software, IT platforms and internet access in accordance with the staff acceptable use policy (AUP) and Trust GDPR Policy.

10. How Linden Lodge School will respond to issues of misuse

Where a student misuses the school's IT systems or internet, we will take action based upon the individual circumstances, nature and seriousness of the specific incident, and this action will be proportionate.

Where a staff member misuses the school's IT 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 where appropriate under the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

11.1 Staff, governors and volunteers

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, newsletters and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
  - Abusive, threatening, harassing and misogynistic messages.
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
  - Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL lead for online safety will undertake child protection and safeguarding training, which will include online safety. They will also update their knowledge and skills on the subject of online safety at regular intervals.

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.

11.2 Students

All students will receive meaningful training on safe internet use, including where appropriate:

- Methods that hackers use to trick people into disclosing personal information

- Password security.
- Social engineering.
- The risks of removable storage devices (e.g. USBs).
- Multi-factor authentication.
- How to report a cyber incident or attack.
- How to report a personal data breach.

Students will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

12. Monitoring arrangements

The Safeguarding team use MyConcern to log safeguarding issues related to online safety.

This policy will be reviewed annually by the online safety lead. At every review, the policy will be shared with the governing board. The review will be supported by an annual assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.