Online Safety

Introduction

The Loddon School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, visitors and trustees.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school in its use of technology, including smart technology; mobile phones and tablets.
- Establish clear mechanisms to identify, intervene and escalate a concern, 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, fake news, 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 them 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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

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

As with all safeguarding-related risks, it is important to consider the risk in the context of the specific needs of children at The Loddon School.

Staff have a duty of care to safeguard and promote the welfare of children and young people, and as technology increasingly permeates every aspect of our lives, staff have a responsibility to deal with potential online safety concerns and to promote safe and responsible behaviour.

Access to the internet on the School Computers, VTrons/Prometheans, tablets and children's own internet devices (e.g., iPad) and mobile phones are restricted to certain sites, using recognised safety software and settings to filter inappropriate sites. Web filtering is applied across all Foundation networks. Additional filtering is in place on the student network. The restrictions are in place to make it less likely of inadvertently placing children at risk. The school runs a monitoring system so all material accessed online is monitored and any concerning use identified can be reported to the safeguarding team.

Roles and responsibilities

Trustees

The trustees have overall responsibility for monitoring this policy and holding the school leaders to account for its implementation.

All trustees 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.
- Ensure that online safety is a running and interrelated theme while devising and implementing a whole school approach to safeguarding and related policies and/or procedures.

Receive training on safe internet use and online safeguarding concerns as part of their safeguarding training.

The Principal

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

Ensure that teaching about online safety is adapted to the needs of the children.

The Designated Safeguarding Lead (DSL)

Details of the school's Designated Safeguarding Lead (DSL) and deputy DSLs are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Principal, IT Manager and other staff, as necessary, to address any online safety issues or concerns.
- Ensure their knowledge and training is up to date on online safety.
- Managing all online safety issues and concerns in line with the school's child protection and safeguarding policy.
- Ensuring that any online safeguarding concerns are reported in accordance with the child protection and safeguarding policy.
- Ensuring staff have awareness of cyber-bullying and report any concerns in accordance with the child protection and safeguarding policy.
- Deliver online safety training including cyber-bullying as part of our safeguarding training, including in induction.
- Understand the filtering and monitoring systems the school use.

- A review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks children face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

The IT Manager

The IT Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems.
- Reviewing and updating this system on a regular basis to assess effectiveness and ensure children are kept 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 system.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring online safety system reviews and changes are logged and dealt with appropriately in line with this policy.
- Along with our contracted IT support company conducting, at minimum, annual checks on the web filtering to ensure it is robust and working correctly. This will be completed as a part of the wider online safety review.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of online safety and adhering to this policy and the mobile and office phone policy when using the school's ICT system and internet.
- Reporting online safety concerns including concern of content on a school device in accordance with this policy and the child protection and safeguarding 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'.
- Staff should ensure the children do not access inappropriate and age-inappropriate content by monitoring the children's use of technology. All staff receive regular safeguarding training, which also highlights the risks of inappropriate use of media, cameras, mobile phones, and computers. They are also reminded about the procedure for reporting concerns. If inappropriate sites are inadvertently accessed staff are duty-bound to report this so that action can be taken to remove these sites.

- Staff are reminded of the privacy and confidentiality of the Loddon children when using the internet, including social media sites in their own time. Staff may not mention children by name, characteristics, or behaviours either in seriousness or in jest. Staff may not upload or post any photos relating to the school or the children onto personal or non-school social media sites, apart from authorised staff using the school-based social media accounts. Staff may not discuss children, other staff, or the school on such sites. Staff need to be aware that others may contact staff through social media sites in order to groom staff and gain access to the children.

Visitors

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 may be expected to agree to the terms of acceptable use policy.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL in line with our child protection and safeguarding policy.

Educating children about online safety

The Loddon School recognises its responsibility to teach children about online safety. The children's risk of online safety is reduced due to their needs and interests. Teaching online safety is delivered at a level appropriate for the children and their level of risk.

How the school will respond to issues of misuse

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 Code of Conduct. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

The DSL will report concerns which involve illegal activity or content, or otherwise serious incidents, in line with the child protection and safeguarding policy.

Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding policy
- Staff disciplinary procedures
- Social Media policy
- Data protection policy and privacy notices
- Mobile and Office Telephones policy

This policy is written to adhere to Keeping Children Safe In Education (KCSIE) 2023 and Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk). There is further guidance and signposting in KCSIE that may inform reviews of this policy and the annual online safety risk assessment review.

Date	**Summary of Changes**	**Date of next review**
September 2023	Writing of this new policy: combined the former TLS policy (the now deleted eSafety policy) and The Key's template policy on the subject. Loddonised the content.	September 2024
10th May 2024	Review – no material change.	May 2025