Lyndhurst School E-Safety Policy

Last Revised	October 2026
Policy Owner	Head of ICT
Date of next review	October 2027

Policy Approval and Sign-Off

Emma Morgan Headmistress Signature *Emma Morgan*

Ed Currie Chair of Governors Signature *Ed Currie*

1. Policy Statement and Scope

This is a whole school policy that applies to all members of Lyndhurst School. The policy covers all members of the school community (staff, learners, visitors, parents, etc.) who use school digital systems, both on and off-site, and includes the use of personal digital technology on the school site where allowed. The school is empowered to regulate the behaviour of pupils when they are off the school site if the behaviour is pertinent to incidents of online-bullying or other online safety incidents linked to membership of the school. Any action taken will be covered by the published Promotion of Positive Behaviour Policy.

Associated Policies and Documents

- Safeguarding and Child Protection Policy
- Promotion of Positive Behaviour Policy and Anti-Bullying Strategy
- ICT Acceptable Use Agreements (AUA) for all user groups
- Data Protection Policy and Privacy Notice
- Keeping Children Safe in Education (2026)
- Technical Security Policy (details technical requirements)
- Cyber Incident Response Plan (CIRP) (details reporting steps)

2. Roles and Responsibilities

All members of the school community are responsible for developing safe and responsible online behaviours and immediately reporting concerns and misuse.

Headmistress, Senior Leaders, and Governors

The Headmistress has a duty of care for ensuring the safety (including online safety) of the school community.

- **Headmistress/SLT:** Responsible for fostering a culture of safeguarding and ensuring the DSL, technical staff, and E-Safety Lead carry out their duties effectively and receive suitable training.
- **Designated Safeguarding Lead (DSL):** Takes the lead responsibility for all safeguarding and child protection, which explicitly includes online safety. The DSL will carry out an internal check of filtering and monitoring logs every half term and submit monitoring reports to the SLT each term.
- **Senior leader for filtering and monitoring:** Emma Morgan (Headmistress and DSL) is the member of the senior leadership team responsible for making sure the DfE filtering and monitoring standards are met. She is also the E-Safety Lead. She works with Unity IT, the school's IT support provider, to check the systems are effective, and leads a full review at least once every academic year.
- **Governors:** Responsible for the approval and review of this E-Safety Policy and for checking that provision (like staff training) is taking place.
- **Safeguarding Governor:** Jo-Ann Atkins is the governor responsible for filtering and monitoring. She works with the DSL to check that the standards are being met and that the annual review takes place.

E-Safety Lead and Technical Staff

- **E-Safety Lead (Emma Morgan, Headmistress and DSL):** Leads the day-to-day management of online safety issues, promotes awareness, manages the logging of incidents, and liaises with technical staff at Unity IT.
- **Network Manager/Technical Staff (Unity IT / Perfect Fit):** Responsible for ensuring the technical infrastructure is secure against malicious attack, enforcing access control, implementing filtering/monitoring systems, and keeping systems patched, all in line with the separate **Technical Security Policy**.

3. Filtering and Monitoring Standards

To meet the statutory requirements of **Keeping Children Safe in Education (2026)**, the school employs the **Smoothwall** platform and clearly defines responsibilities for its appropriate use.

- **Prohibited Content:** Internet access is filtered for all users. Illegal content, specifically child sexual abuse images, is actively filtered by employing the **Internet Watch Foundation Child Abuse Image Content (CAIC) list**. Filtering and monitoring standards also ensure children are safe from **terrorist and extremist material**.
- **System Responsibility: Smoothwall** is the dedicated third-party system used to regularly monitor and record the activity of users on the school technical systems. Unity IT, the school's IT support provider, applies and maintains the filtering settings. The E-Safety Lead checks the filtering standards and agrees any updates with Unity IT, so that they are applied and updated on a regular basis.
- **Preventing Subversion:** Systems and acceptable use agreements are in place to prohibit the use of proxies or other mechanisms to bypass the filtering or other safeguards employed by the school.
- **Log Review and Triage:** The **Designated Safeguarding Lead (DSL)** is responsible for reviewing the monitoring logs every half term to ensure timely action is taken against potential risks. There is a clear process in place to deal with requests for filtering changes, which must be approved by the E-Safety Lead (the DSL).
- **Annual Review:** The filtering and monitoring provision is reviewed at least once every academic year, across all school devices and locations, and more often if there is a significant change or a safeguarding concern. A record of each review and check is kept on the school's safeguarding drive.
- **User Awareness:** All users are made aware of the use of monitoring software and logging of their internet use through the acceptable use agreement.

4. Education, Communications, and Incident Management

Education and Training

- **Pupils:** Online safety is a focus across the curriculum, specifically through Computing and PSHE. Pupils are taught to be critically aware of online content and understand the importance of reporting abuse.

- **Staff and Governors:** All staff receive online safety training at induction and as part of their termly safeguarding training, including their role in filtering and monitoring and how to report concerns. Governors receive safeguarding and child protection training, including online safety, at induction and regularly after that.
- **Parents and Carers:** The school sends a termly safeguarding newsletter to parents and carers, which highlights popular apps and current online concerns and gives practical tips for keeping children safe online.
- **Screen Time:** The school has screen time guidance for staff, covering the use of screens with pupils, and for parents and carers, covering screen use at home.

Communications and Image Use

- **Digital Communications:** All communications between staff and children or parents/carers must be **professional** in tone and content and must only take place on **official (monitored) school systems**. Personal email addresses or social media must not be used for these communications.
- **Digital Images:** Staff must **only use Lyndhurst School equipment** for taking images to support educational aims. Parents are welcome to take videos and images of their own children at school events for personal use but **must not publish these images or comment on other pupils** on social networking sites.
- **Social Media:** Staff must ensure **no reference** is made in social media to children, parents/carers, or Lyndhurst School staff.

Real-Time Media and Social Media Sharing

To ensure the safeguarding and privacy of our pupils in accordance with UK GDPR, the school strictly regulates the real-time sharing of images and videos on social media platforms. We will not broadcast or post real-time media, nor will we disclose the immediate locations of children, while they are off-site on routine school trips or excursions. The sharing of live or real-time updates is exclusively permitted for events held securely on the school site, or during large-scale, off-site school events and sports fixtures (e.g., Sports Day). In all permitted instances, the publication of such media remains subject to the school's overarching data protection protocols and standard parental consent agreements.

Data Security and Incident Response

- **Data Protection:** The school complies with data protection law as detailed in the separate **Data Protection Policy**. Personal data breaches that must be reported are reported to the Information Commissioner's Office (ICO) within 72 hours of the school becoming aware of them.

- **Incident Response:** Any online safety concern about a child must be reported to the DSL or a Deputy DSL straight away and logged on My Concern. Illegal incidents, such as accessing child abuse images, must be **immediately referred to the Police. Staff must never view, copy, forward or delete such images, and must follow the Safeguarding and Child Protection Policy**. All other incidents of misuse are recorded and dealt with through normal disciplinary procedures, in line with the separate **Promotion of Positive Behaviour Policy** and **Staff Code of Conduct**. The detailed steps for handling and escalating a technical or data breach incident are contained within the school's **Cyber Incident Response Plan (CIRP)**.

5. Online Risks, Artificial Intelligence and Devices

Understanding online risk

In line with KCSIE 2026, the school considers online safety under four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material, such as pornography, misinformation, racism, misogyny, self-harm, suicide, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users, such as grooming, or adults posing as children.
- **Conduct:** online behaviour that increases the likelihood of, or causes, harm, such as making, sending or receiving explicit images, or online bullying.
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and financial scams.

These risks are covered in Computing and PSHE lessons and in staff training.

Artificial intelligence (AI)

Pupils may only use AI tools in school that the school has approved, under adult supervision, and the school's filtering and monitoring apply to them. Pupils are taught that AI can produce content that is wrong, biased or harmful, and that creating or sharing fake images, videos or messages of other people is never acceptable. Any AI-generated image of a child that is nude or sexual is a safeguarding concern and must be reported to the DSL immediately.

Staff must not enter personal information about pupils, parents or colleagues into AI tools that the school has not approved, and they remain responsible for checking anything AI produces before using it.

Mobile phones and personal devices

Lyndhurst is a phone-free school. Pupils do not use mobile phones, smart watches or other personal digital devices during the school day. Any phone a pupil brings to school is handed in at the front reception on arrival and collected at the end of the day. The only exception is a device a child needs for a medical condition, agreed in advance as part of their individual healthcare plan or EHCP. Further detail is in the Promotion of Positive Behaviour Policy and the Safeguarding and Child Protection Policy, which also sets out the rules on staff phones and cameras in the Early Years.

Cyber-bullying and online abuse

Cyber-bullying is dealt with under the Anti-Bullying Strategy. The sharing of nude or semi-nude images, online sexual harassment and other online child-on-child abuse are dealt with under the Safeguarding and Child Protection Policy.