Lyndhurst School E-Safety Policy

Last Revised	September 2025
Policy Owner	Head of ICT
Date of next review	September 2026

Policy Approval and Sign-Off

Andrew Rudkin Headmaster Signature *Andrew Rudkin*

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 Behaviour Policy.

Associated Policies and Documents

- Safeguarding and Child Protection Policy
- Behaviour Policy and Anti-Bullying Policy
- ICT Acceptable Use Agreements (AUA) for all user groups
- Data Protection Policy and Privacy Notice
- Keeping Children Safe in Education (2025)
- 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.

Headteacher, Senior Leaders, and Governors

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

- **Headteacher/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.
- **Governors:** Responsible for the approval and review of this E-Safety Policy and for checking that provision (like staff training) is taking place.

E-Safety Lead and Technical Staff

- **E-Safety Lead:** Leads the day-to-day management of online safety issues, promotes awareness, manages the logging of incidents, and liaises between the DSL and technical staff.
- **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 (2025)**, 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. Technical staff ensure the filtering standards 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/academy.
- **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.
- **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 PHSCE. 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 Governors are expected to participate in appropriate awareness sessions.

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 GDPR requirements, 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**. Breaches are reported to the Information Commissioner within 72 hours of becoming aware.
- **Incident Response:** Illegal incidents, such as accessing child abuse images, must be **immediately referred to the Police**. All other incidents of misuse are recorded and dealt with through normal disciplinary procedures, in line with the separate **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)**.