LALEHAM LEA

A Catholic Independent Primary School for boys and girls aged 3 to 11

Headteacher: Mrs. M Reece

# LALEHAM LEA SCHOOL & NURSERY

# ONLINE SAFETY POLICY (E-Safety)

*This is a whole school policy which applies to all sections of the school, including Early Years Foundation Stage, Out of School Care and Clubs.*

| | Date | Signed |
|---|---|---|
| Date reviewed | September 2026 | *M Reece* Headteacher |
| Ratified by the Board of Governors | October 2026 | Y Epale Chair of Governors |
| Date of next review | October 2027 | |

(If at any time circumstances or situations change in this subject area then the policy will be reviewed earlier)

***Mission Statement:***

*Recognising that Christian values are central to the life of the school, we at Laleham Lea aim to create a loving, welcoming safe environment in which our children may grow intellectually, socially and emotionally; an environment in which their talents are recognised and fostered and their differences treated with compassion; an environment which provides quality teaching and learning within a balanced curriculum framework and which helps every child to reach their true potential. Together with parents, who are the first educators, we aim to lead our children towards tolerance, understanding and sensitivity to the needs of others so that they may grow up as well-balanced individuals with a strong sense of personal identity and an awareness of God's love.*

## 1. Aims

This policy aims to:

- Set out expectations for all Laleham Lea's School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching and learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (see Behaviour Policy, Anti-Bullying Policy, Child Protection & Safeguarding Policy, Whistleblowing Policy)
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
  - for the protection and benefit of the children and young people in their care, and
  - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
  - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- This policy applies to pupils and all parents, visitors and staff at Laleham Lea; including the governing body, leadership teams, teachers, support staff, external contractors, volunteers and other individuals who work for, or provide services to our school.

This policy was written with regard to:

- Keeping Children Safe in Education, 2026;
- Using Technology in Education, 2019 (updated June 2025)
- Meeting Digital and Technology Standards in schools and colleges, 2022 (updated March 2025)
- Generative Artificial Intelligence in Education (2025)
- Early Years and Foundation Stage Framework
- Working Together to Safeguard Children, 2023;
- Behaviour in Schools: Advice for Headteachers and school staff, 2022;
- Teaching Online Safety in Schools, 2019 (updates January 2023)
- Education for a Connected World framework - 2020.

This policy should be read in conjunction with:

- Safeguarding policy
- Anti-Bullying policy
- Behaviour policy
- The staff handbook
- Curriculum policies, such as: Personal Social Health and Economic Education (PSHE) and Relationships and Sex Education (RSE)

## 2. Introduction

Technology and communications are rapidly changing and becoming more sophisticated. With this change come new ways of being unsafe and feeling threatened. Online Safety has become a very important issue which it is essential to address in school throughout different areas of the curriculum to ensure that all children and adults remain safe and in control when using technology. This could be either using mobile telephones or computers or other mobile devices with access to the internet

We aim to help every pupil and adult to:

- Feel safe and confident when using new technologies.
- Know who to speak to when they unsafe.
- Know how to report any abusive behaviour.
- Know how to use the internet correctly, without misuse.
- Stay in control and keep personal information private.
- Understand how to take the necessary measures to block and delete accounts, messages and people.

Implementation:

There are two main features of the implementation of this policy:

1. *Prevention*: robust and responsive systems for filtering and monitoring online activity.

2. *Education*: training users to be responsible, discerning and considerate whilst online.

Staying safe online requires a multi-layered approach which includes filtering, monitoring, education, clear consequences and pastoral support. It would not be in the educational interest of our pupils to block the internet entirely and so we rely on all users to engage with regular and effective communication regarding online safety so we can use the internet to achieve the best possible educational outcomes whilst also keeping everyone safe

## 3. Roles and Responsibilities

The Designated Safeguarding Lead (DSL) has lead responsibility for online safety and filtering and monitoring. While activities of the designated safeguarding lead may be delegated to appropriately trained deputies, the ultimate lead responsibility for safeguarding and child protection remains with the DSL. In accordance with KCSIE 2026, this lead responsibility for online safety and understanding filtering and monitoring systems and processes is explicitly included within the DSL's job description.

The DfE digital and technology standards and KCSIE 2026 require the governing body to identify and assign a named member of the Senior Leadership Team (SLT) and a named Governor to be responsible for ensuring filtering and monitoring standards are met and reviewed.

We recognise that all members of the school community have important roles and responsibilities to play regarding online safety.

### Governors

The Governors are responsible for:

- Exercising overall strategic responsibility for approving the Online Safety Policy and ensuring its effectiveness is reviewed at least once every academic year in accordance with statutory KCSIE 2026 requirements.
- Identifying a named Governor responsible for overseeing filtering and monitoring standards.
- Ensuring the school has appropriate filtering and monitoring systems in place across all school-owned devices, networks, and backup connections.
- Ensuring that filtering and monitoring arrangements are documented, and receiving regular assurance reports from the named SLT lead and DSL.
- Carrying out regular monitoring of Online Safety incident logs, filtering breach reports, and filtering/monitoring review records.

**Headteacher and Senior Leadership Team (SLT)**

The Headteacher and SLT are responsible for:

- Assigning a named member of the SLT to hold operational leadership responsibility for filtering and monitoring reviews, working in close collaboration with the DSL and technical support.
- Ensuring online safety is treated as a core safeguarding issue in line with national recommendations and KCSIE 2026, embedded as a running theme across the whole-school safeguarding approach.
- Scoping the school's specific digital needs, documenting block and allow decisions, and ensuring that filtering and monitoring mechanisms address emerging digital risks, including Generative AI (e.g., AI chatbots, companion systems, deepfakes, and non-consensual image generation).
- Conducting regular filtering checks across all internet-connected devices and locations, and maintaining written records of all filtering checks as required by KCSIE 2026.
- Ensuring DfE Filtering and Monitoring Standards and digital technology standards are fully met, utilizing the DfE guidance *Generative AI: Product Safety Expectations*.
- Ensuring all staff receive regular, updated online safety and safeguarding training that explicitly covers their specific roles and escalation responsibilities relating to filtering and monitoring.
- Supporting the DSL and deputies by providing adequate time, funding, training, and resources to carry out their online safeguarding duties effectively.
- Auditing and evaluating online safety practice annually to identify gaps, trends, and areas for improvement.

**Online Safety Lead (Designated Safeguarding Lead - DSL)**

The DSL (a senior member of the SLT) is responsible for:

- Taking lead responsibility for online safety and ensuring this requirement is explicitly detailed within their formal job description.
- Maintaining a thorough understanding of the school's filtering and monitoring systems, processes, and alert thresholds.
- Overseeing and reviewing filtering and monitoring alerts and reports (e.g., Smoothwall), ensuring prompt investigation and appropriate safeguarding responses.
- Working alongside Deputy DSLs, SENCOs, pastoral staff, and external IT support (Virtual IT) to coordinate online safeguarding.
- Maintaining formal records of all online safety concerns and filtering/monitoring incidents within the school's safeguarding recording system.
- Addressing risks across the updated 4 Cs framework (Content, Contact, Conduct, Commerce), including Generative AI risks (AI chatbots, AI companions, voice cloning, disinformation, and the making or sharing of nudes and semi-nudes including deepfakes).
- Accessing regular, specialist training regarding online risks, filtering and monitoring, and the unique online vulnerabilities of SEND learners and vulnerable children.

- Reporting online safety data, trends, and compliance updates regularly to the Headteacher and Governing Body.

**Technical Staff / External IT Provider (Virtual IT)**

The Network Manager / External IT Provider is responsible for:

- Providing technical support to the SLT and DSL to implement and maintain compliant filtering and monitoring systems (including Smoothwall monitoring and Virtual IT filtering).
- Ensuring filtering blocks all content on the Internet Watch Foundation (IWF) list and Counter Terrorism Internet Referral Unit (CTIRU) list across all networks, backup connections, and devices.
- Assisting SLT and DSL in conducting annual filtering and monitoring reviews, and **maintaining written logs/records of all technical testing checks across all devices and locations**.
- Ensuring systems can filter and monitor emerging threats, including Generative AI platforms, VPN/proxy bypass tools, and mobile/app content.
- Reporting technical filtering breaches or system failures immediately to the DSL and SLT.
- Ensuring infrastructure security, password enforcement, multi-factor authentication (2FA) for administrative accounts, and system updates in line with DfE Cyber Security Standards

**Teaching and Support Staff**

Teaching and Support Staff are responsible for:

- Reading Part One of KCSIE 2026 in full (noting the removal of Annex A) and adhering to the Online Safety Policy, Staff Code of Conduct, and Acceptable Use Policies.
- Understanding that technology is an integral part of safeguarding, recognizing that online abuse and face-to-face abuse frequently occur concurrently.
- Understanding their specific responsibilities regarding filtering and monitoring, including knowing how to escalate concerns such as:
    - Witnessing or suspecting access/creation of unsuitable or illegal material.
    - Software/system failures or attempts by pupils to bypass filtering/monitoring.
    - Teaching planned topics that may generate unusual activity in filtering logs.
    - Perceived unreasonable restrictions that hinder teaching and learning (over-blocking).
- Being alert to emerging digital risks, including AI-generated deepfakes, AI chatbots, and the making or sharing of nudes and semi-nudes.
- Proactively monitoring learner device use during lessons and modelling exemplary digital conduct.
- Embedding age-appropriate online safety education throughout the curriculum.

**Pupils**

Pupils are responsible for:

- Engaging in age-appropriate online safety education delivered through ICT, PSHE, and assemblies.
- Using school digital technologies and devices strictly in accordance with the Pupil Acceptable Use Policy.
- Understanding expectations regarding personal mobile devices and smartwatches (noting that personal electronic devices and smartwatches are strictly prohibited on school premises and trips).
- Respecting others online and offline, recognizing the harms of cyberbullying, harassment, and sharing inappropriate or AI-generated content.
- Immediately reporting any online safety concern, upsetting content, or filtering breach to a trusted adult or via the school website's 'Report Abuse' channel.

**Parents / Carers**

Parents and carers are responsible for:

- Supporting the school in promoting safe and responsible online behaviour at home.
- Partnering with the school by attending online safety information sessions and reviewing guidance materials provided in newsletters and on the school website.
- Ensuring children use mobile phones and personal devices appropriately outside of school, keeping devices at home in line with school policy.
- Informing the school immediately if they or their child encounter online safeguarding risks or concerns involving the school community.
- Adhering to school guidelines regarding the appropriate capture and sharing of digital images at school events.
- They must be aware of the schools Acceptable Use Policy and agree to it (Appendix 2).

## 4. Education

**Pupils** -

All pupils receive planned, progressive online safety education embedded across the ICT/Computing and P.S.H.E. lessons, supplemented by regular assemblies and national awareness campaigns (such as *Safer Internet Day*). Schemes of work are regularly updated to reflect new and emerging digital technologies, online behaviours, and risks both inside and outside of school.

Key elements of the pupil curriculum include:

- Teaching pupils to understand, recognise, and critically evaluate AI-generated content. This includes age-appropriate awareness of deepfake images/videos, voice cloning, digital manipulation, and the ethical, personal, and legal consequences of generating or sharing altered media.

- Educating pupils on safe interactions with AI-powered tools, AI chatbots, search-embedded AI, and companion-style applications, highlighting data privacy, emotional boundary risks, and automated interactions.

- Educating pupils on the risks and legal implications of creating, requesting, or sharing explicit images **("Nudes and Semi-Nudes)**, explicitly incorporating AI-altered, synthetic, or AI-generated non-consensual imagery.

- Teaching pupils across all key stages to critically evaluate online content, question the validity of digital information, and verify source accuracy before sharing or relying on information.

- Differentiated and ability-appropriate online safety education is provided for vulnerable pupils, including Looked After Children (LAC), pupils with Special Educational Needs and Disabilities (SEND), English as an Additional Language (EAL) learners, EYFS children, and those experiencing trauma or loss. Staff recognise that children with cognitive or communication difficulties may struggle to distinguish fact from fiction in online/AI content and provide tailored scaffolding to prevent unintentional misuse or repetition of harmful behaviours.

- **Supervised Digital Learning:**
    - *EYFS & Key Stage 1:* Internet access occurs via adult demonstration and close, direct supervision on pre-approved materials supporting specific learning outcomes.
    - *Key Stage 2:* Pupils use age-appropriate search tools under staff supervision. In pre-planned internet tasks, staff direct pupils to checked resources. Where free searching occurs, staff actively monitor pupil screens and online activity.

**Parents** -

Many parents and carers have only a limited understanding of online safety, risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Parents will be invited to attend Online Safety meetings, where they will also have the opportunity to ask questions regarding Online Safety. They may also receive information at parents' evenings and by newsletters and the school website.

The school will ensure parents have been given information of the relevant web sites/publications e.g.

- SWGfL (swgfl.org.uk)
- UK Safer Internet Centre (saferinternet.org.uk)
- Childnet Parents & Carers (childnet.com/parents-and-carers)

- National Online Safety (NOS) Parent App

The School will ensure parents review and agree to the Pupil Acceptable Use Policy (Appendix 2) and provide clear reporting channels if parents or their children encounter online risks affecting the school community

**Staff Professional Development (CPD) & Induction**

All staff must recognise technology as an integral component of safeguarding and be equipped to protect pupils across both physical and digital environments.

Key elements of staff training and CPD include:

- **Mandatory Statutory Reading (KCSIE 2026):** Following the removal of Annex A in KCSIE 2026, **ALL members of staff are required to read and understand Part One of Keeping Children Safe in Education ("Safeguarding Information for All Staff") in full** upon joining the school and at the start of each academic year.

- **Induction & Annual Training:** All new staff complete online safety training during induction. All existing staff complete formal annual CPD (utilising platforms such as TES Develop and local authority updates), covering:

    - Whole-school safeguarding policy updates and staff roles.
    - Staff Acceptable Use Policy (Appendix 1) and Staff Code of Conduct.
    - **Filtering & Monitoring Responsibilities:** Practical training on how filtering (Virtual IT) and monitoring (Smoothwall) operate, recognising system failures or bypass attempts (e.g., VPNs, proxy sites, "unblocked AI" portals), and exact internal reporting and escalation pathways.
    - **Emerging Digital Risks and Generative AI:** Guidance on identifying and responding to risks involving AI chatbots, AI-generated nudes and semi-nudes, deepfakes, voice cloning, and online harassment/cyberbullying.
    - **Professional Online Conduct:** Reinforcing expectations that staff act as positive digital role models, maintain strict professional boundaries on personal social media, use work-issued devices exclusively for professional purposes, and remain aware that all activity on school systems is monitored and traceable.
    - **Classroom Best Practice:** Safe digital teaching methodologies, pre-checking internet sites, active classroom supervision, and reporting unsuitable search results for technical blocking.

## 5. Safer Use of Technology

**Classroom Use**

- We use a wide range of technology. This includes access to:

- Chromebooks, tablets and other digital devices
- Internet which may include search engines and educational websites
- Learning platform/intranet (remote teaching is needed)
- Email
- Digital cameras, web cams and video cameras

- All devices will be used in accordance with our Acceptable Use Policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of learners will be appropriate to their age and ability.
  - Early Years Foundation Stage and Key Stage 1
    Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.
  - Key Stage 2
    Learners will use age-appropriate search engines and online tools and only in the presence of a member of staff.
    Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.

**Managing Internet Access**

All staff, learners and visitors will read and sign an Acceptable Use Policy before being given access to our computer system, IT resources or internet.

**Filtering and Monitoring**

Laleham Lea School recognises the importance of robust filtering and monitoring procedures as stipulated in KCSIE. The school is compliant with the DfE's filtering and monitoring standards for schools and colleges. This is checked and reviewed at least annually using the checklist appended to this policy.

- Our governors and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- We follow the guidance outlined in the DfE filtering and monitoring standards
- Changes to the filtering and monitoring approach will be risk assessed by the Senior Leadership Team

- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate and these are recorded (appendix 5)
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

At Laleham Lea we utilise the services of Virtual IT to filter online usage, and Smoothwall to monitor our online activity.

Filtering:

- Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video (DFE: Meeting Digital and Technology Standards in Schools and Colleges 2022, updated 2025)
- Virtual IT filters content by category, has a block and allow list (which allows us to add/remove access to specific websites) and can also filter by keyword allowing for an extremely targeted approach.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g., discrimination, weapons- which could be part of a study on the Roman Army) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (Virtual IT) can temporarily remove those sites from the filtered list for the period of study, only after discussion with the Online Safety Lead.
- It should be noted that no filtering system is 100% effective – to allow educational use of the internet, not all available categories (advertising, image hosting etc.) can be blocked as most websites will fail to load. There may be times where a child can get to a site that the teacher would deem inappropriate – if this happens, the website should be reported to the Virtual IT Helpdesk by email with the subject title “Website Reclassification” to ensure that site is filtered promptly. breach will be recorded and escalated as appropriate. Parents/carers will be informed of filtering breaches involving their child.
- Virtual IT filtering is active on pupil chrome books, classroom desktop computers and staff laptops. When staff log in with their own credentials, web filtering is aligned to their access rights, for example, admin staff can access more than student users.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- The filtering system blocks all sites on the Counter Terrorism Internet Referral Unit (CTIRU) list.

Monitoring:

- Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity (DFE: Meeting Digital and Technology Standards in Schools and Colleges 2022, updated 2025)
- Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. Technical monitoring solutions rely on software applied to a device that views a user’s activity.

- Smoothwall offers technical monitoring and it monitors all internet usage on Laleham Lea devices.
- Smoothwall is a real-time content-aware analysis. It monitors every button pressed on our school devices, including pupil chrome books, staff desktops in classrooms and staff laptop devices. It scans the content and context of every page for unwanted material and has 120 filtering categories which can be used to tailor the web browsing experience of all audiences to ensure that harmful content is out of reach.
- The DSL and DDSL receive a weekly Smoothwall monitoring report outlining the activity of individuals, both staff and pupils and whether any inappropriate content has been searched for or accessed. Monitoring data can be reviewed on the Smoothwall administration portal. The DSL is responsible for overseeing the regular review of this information and acting accordingly.
- All staff and pupils will be made aware that there is also a monitoring system in place and any online activity can be traced.

**Security and Management of Information Systems**

We take appropriate steps to ensure the security of our information systems, including:

Further information is available in the DfE cybersecurity standards:

https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-andcolleges/cyber-security-standards-for-schools-and-colleges

- Protecting all devices on every network with a properly configured boundary or software firewall
- Keeping an up-to-date list of every device that is able to access the network and ensuring their security features are enabled, correctly configured and up to date
- Ensuring that accounts only have the access that they require to perform their role and should be authenticated to access data and services
- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments. o Regularly checking files held on our network,
- The appropriate use of user logins and passwords to access our network.
- Specific user logins and passwords will be enforced for all but the youngest users.
- All users are expected to log off or lock their screens/devices if systems are unattended.

**Passwords**

- All members of staff will have their own username and passwords to access our systems; members of staff are responsible for keeping their password private.

- From Year 1 all learners are provided with their own username and passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to:
  - Use strong passwords for access into our system.
  - Use a separate password for your work and personal accounts.
  - Always keep their password private; users must not share it with others or leave it where others can find it.
  - Not to login as another user at any time.
  - Use two-factor/two-step verification for all accounts which have access to personal or sensitive operational data and functions.
  - Store passwords securely

**Managing the Safety of our Website**

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our school address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.

**Publishing Images and Videos Online**

We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: Acceptable Use Policies, Codes of Conduct/Behaviour, Child Protection and Safeguarding and parental media consent

**Managing Email**

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including Acceptable Use Policies and the Code of Conduct/Behaviour Policy.
- Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately inform the DSL/DDSL if they receive offensive communication, and this will be recorded

**Staff Email**

- The use of personal email addresses by staff for any official school business is not permitted.
- All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

## 6. Technical Security Procedures

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The IT provider and IT lead are to be responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access.
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the data protection policy.

**Technical Security Overview**

- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- All users will have clearly defined access rights to school technical systems. Details of any elevated access rights available to user will be recorded by the Headteacher and will be reviewed, at least annually.
- Users are responsible for the security of their username and password, must not allow other users to access the systems or Wi-Fi using their login details and must immediately report any suspicion or evidence that there has been a breach of security.
- School Staff will not install software without the permission of the Headteacher
- Where available, guest Wi-Fi "Passes" can be granted by the school administration team without referring to the SBM, however, this only gives temporary internet access, not any access to the school systems.
- Any device provided by the school is for school use only – family members/friends should not attempt to use the device, unless for the reason of helping a child (who is the assigned keeper of the device). Any personal use by the assigned keeper of the device is liable to be monitored.
- The school infrastructure and individual workstations are protected by up-to-date antivirus software to protect against malicious threats from viruses, worms, trojans etc.
- All personal data will be stored on the school server only (which is virus and malware protected) according to the Data Protection Act 2018. Staff must access personal data via secure password

protected machines and devices only, ensuring that they 'log off' at the end of any session to minimise any chance of the data being seen by others.

## 7. Use of Digital Video and Images

The development of digital images and videos offers significant benefits within the curriculum and enhances learning. Images and videos may be captured by staff and pupils for educational purposes or accessed online to support classroom activities. However, all members of the school community must be fully aware of the risks associated with taking, editing, and sharing digital images online.

Staff and pupils are educated to understand that once content is published online, it can remain permanently accessible and be copied, manipulated, or shared without consent, potentially causing severe long-term harm or distress.

Digital Video and Images

- Education and Awareness: Staff will inform and educate pupils about the risks attached to capturing, using, publishing, and distributing digital images, including the misuse of personal images on social networking platforms.
- Equipment Use: Staff are permitted to take digital or video images solely to support official educational outcomes. All images must be taken using school-owned equipment only; the use of personal cameras, phones, or devices by staff for capturing pupil images is strictly prohibited.
- Appropriate Capture: Staff must ensure that all pupils are appropriately dressed and engaged in suitable activities before any photo or video is taken.
- Pupil Privacy: Pupil full names will never be published alongside photos or videos on the school website, blogs, or public communication channels.
- Parental Consent: Written media consent must be obtained from parents/carers upon entry to the school before any images or videos of pupils are published online or in promotional materials.
- Data Protection: The school strictly adheres to the Data Protection Act 2018 and UK GDPR in the collection, storage, and processing of all digital imagery.

## 8. Mobile Phones

Laleham Lea School fully complies with DfE statutory guidance *Mobile phones in schools (2026)* to maintain a safe, focused environment free from digital distraction, cyberbullying, and online risks.

**Expectations**

All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as Anti-bullying, Behaviour, Safeguarding and Child Protection and Staff Code of Conduct.

Electronic devices of any kind that are brought onto site are the responsibility of the user.

- All members of our community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- All members of our community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

Mobile phones and personal devices are only allowed to be used in the staff room and areas when there are no children present, in case of emergency or unless in exceptional circumstances.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour Policy.

All members of our community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

**Staff Use of Personal Devices and Mobile Phones**

- Staff are permitted to bring personal mobile phones onto site, but they may **only** be used in designated staff areas (e.g., staff room) when pupils are not present, or in exceptional emergency circumstances approved by the Headteacher.
- Laleham Lea School is a designated **Mobile Phone Free Site** for staff in all pupil-facing environments.
- Personal devices must be kept switched off or on silent and stored securely in bags/lockers during teaching periods.
- Bluetooth, 'AirDrop', and wireless sharing functions must be disabled while on school grounds.
- Staff are strictly forbidden from using personal devices to contact pupils or parents/carers.
- Any breach of mobile device guidelines by staff will trigger disciplinary procedures under the Staff Code of Conduct. If a device is suspected to contain illegal content or evidence of a criminal offense, law enforcement will be contacted immediately.

**Learners' Use of Personal Devices and Mobile Phones**

In compliance with DfE statutory guidance *Mobile phones in schools (2026)*, Laleham Lea School strictly prohibits pupils from bringing personal mobile phones, digital cameras, or smartwatches (including any 3G/4G/5G-enabled wearable technology) onto school premises.

Pupils are prohibited from bringing mobile phones, electronic devices, or smartwatches with imaging/sharing capabilities on local trips or residential outings. Official photographs are taken exclusively on school-owned equipment by designated staff.

**Visitors' Use of Personal Devices and Mobile Phones**

- Visitors, parents, contractors, and volunteers must abide by the school's Acceptable Use Policy and mobile phone restrictions.
- Clear signage is displayed at all site entrances informing visitors that mobile phone use is prohibited in areas where children are present.
- Staff will challenge any visitor seen using a mobile device in unauthorised areas and report the breach immediately to the DSL or Headteacher.

## 9. Unsuitable Use, Sanctions and Reporting

All users are expected to demonstrate safe, legal, and responsible digital conduct. Infringements—whether accidental or deliberate—will be addressed promptly, proportionately, and rigorously.

**Illegal and Inappropriate Activity**

Users must not access, create, upload, download, generate, share, or transmit any material on school equipment or via personal devices (on or off site) that involves any of the following activities:

Illegal Activities

1. **Making or Sharing of Nudes and Semi-Nudes:** Creating, soliciting, possessing, or distributing explicit images or videos of children, including youth-produced sexual imagery, synthetic/AI-generated nudes or semi-nudes, deepfakes, and non-consensual altered imagery.
2. **Child Sexual Abuse Material (CSAM) & Exploitation (CSAE):** Accessing, storing, or transmitting child sexual abuse material or engaging in child sexual exploitation.
3. **Grooming:** Facilitating, inciting, or arranging sexual acts or unlawful contact against children (Sexual Offences Act 2003).
4. **Extreme Pornography and Illegal Content:** Possessing or distributing extreme pornographic material (Criminal Justice and Immigration Act 2008).
5. **Hatred and Extremism:** Distributing criminally racist or hate-based material, inciting religious/homophobic hatred (Public Order Act 1986), or promoting terrorism and violent extremism in violation of the Prevent Duty.

Prohibited Inappropriate Activities & AI-Generated Harassment

1. **AI-Generated Abusive Content:** Creating, manipulating, or sharing non-consensual AI deepfakes, AI voice cloning impersonations, automated harassment, or digitally altered media designed to humiliate, harass, or defame any individual.
2. **Cyberbullying and Harassment:** Threatening, abusive, discriminatory, or derogatory behaviour targeting pupils, staff, or community members.
3. **Pornography & Unsuitable Content:** Accessing adult content, sexually explicit material, violent content, or material promoting self-harm, suicide, or substance abuse.
4. **Filter & Safeguard Bypassing:** Utilising VPNs, web proxies, anonymisers, "unblocked AI" portals, or technical mechanisms to circumvent school filtering or security controls.
5. **Commercial & Unlawful Misuse:** Running private businesses on school systems, gambling, non-educational gaming, or violating copyright/software licensing laws.
6. **Data & Cyber Security Breaches:** Sharing passwords, accessing unauthorised files/accounts, propagating malware/viruses, or intentionally congesting the network.

Reporting Incidents and Misuse

- Clear reporting procedures are established across the school community. Staff must report any online safety, filtering, or monitoring concerns immediately to the Online Safety Lead / DSL.
- Pupils are taught how to report upsetting or harmful online content to a trusted adult in school, their parents, or via the 'Report Abuse' button on the school website.
- All incidents of online misuse, filtering breaches, or digital safeguarding concerns must be formally recorded on the Online Safety Incident Log (Appendix 3) and transferred to the school's central safeguarding software.

Investigating and Sanctions

- The Online Safety Lead and DSL will investigate all reported incidents. Technical evidence will be gathered in collaboration with technical support (Virtual IT and Smoothwall monitoring logs).
- Misuse arising from carelessness will involve re-education, parental notification, and proportionate sanctions under the Behaviour Policy. Deliberate or severe misuse will lead to formal disciplinary action, withdrawal of IT privileges, suspension, or exclusion.
- Where illegal activity or serious harm is identified (such as the creation or distribution of nudes/semi-nudes, deepfakes, or grooming), the Headteacher and DSL will immediately report the matter to the Police, Children's Social Care, and the Local Authority Designated Officer (LADO).

## 10. Working with Parents

Our school seeks to work in partnership with parents to provide effective Online Safety. Parents need to know that the school's Online Safety programme will complement and support their role as parents and that they

can be actively involved in the determination of the school's policy. Parents will be sent online safety updates via the School Newsletter and/or direct online safety newsletters.

**Appendix 1 – Staff Acceptable Use Agreement form**

**LALEHAM LEA SCHOOL**

## Rules for Responsible Internet Use

ICT Acceptable Use: Agreement form

EMAIL / INTERNET / INTRANET / NETWORK USAGE POLICY

- I will only use the school's Email / Internet / Intranet for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not browse, download or send material that could be considered offensive to colleagues or children.
- I will report any accidental access to inappropriate materials to the appropriate line manager.
- I will not download any software or resources from the Internet that can compromise or damage the network, or is not adequately licensed.
- I will ensure all documents are saved, accessed and deleted appropriately.
- I will not connect a computer or laptop to the network / Internet that does not have up-to-date version of anti-virus software.
- I will not use personal digital cameras or mobile telephone cameras for transferring images of pupils or colleagues without permission from the Head Teacher.
- I will ensure I am aware of digital safe-guarding issues so they are appropriately applied in my classroom practice.
- I will not allow unauthorised individuals to access Email / Internet / Intranet.
- I understand that all Internet usage will be logged and this information could be made available to the Head Teacher and Governing Body on request.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will not use my mobile telephone when in class or in charge of pupils. I will only use my mobile telephone during my personal breaks, or with the express permission of my line manager in emergencies.
- I understand that failure to comply with the Usage Policy could lead to disciplinary action.
- I will exercise discretion when using Social Networking Websites and will notify the Head Teacher immediately if I am contacted by pupils or former pupils of the school. I will not respond to any contact made to me electronically by any child.
- I will notify the Head Teacher if, when using the internet, I recognise any children from school using Social Networking Websites inappropriately or illegally.

User Signature

I have read and understood the E-Safety policy.

I agree to abide by the above Acceptable Usage Policy.

Signature ..... Date .....

Full Name .....(printed)

Job title .....

Authorised Signature (Head Teacher) .....

Is this member of staff temporary? NO / YES

If yes, contract end date: .....

I approve this email account / connection to the Internet / Intranet.

Signature .....

Date .....

Full Name .....(printed)

One copy is retained by member of staff / Second copy for school file

Data Protection Statement
All personal information provided to the school is held in accordance with the Data Protection Act 2018. For more information about Laleham Lea's privacy policy please refer to http://www.lalehamlea.co.uk /sites/default/files/policies/Data-Protection-Policy.pdf

## Appendix 2 Pupil Acceptable Use Policy

LALEHAM LEA SCHOOL

### Rules for Responsible Internet Use

**Please note, this document must be returned signed, to the office before your child will be allowed to use the internet. This agreement will be updated annually.**
**PLEASE KEEP A COPY FOR YOUR INFORMATION**

The school has computers with internet access to help learning.
These rules will help keep us safe and help us to be fair to others. We suggest that you use these rules at home to stay safe.

**Using the computers:**

- I will only access the computer system with the login and password I have been given
- I will not look at or delete other people's files
- I will not bring files into school without permission

**Using the Internet:**

- I will ask permission from a teacher before using the internet
- I will only use the internet when an adult is present in the classroom
- I will report any unpleasant material to my teacher immediately because this will help protect other pupils and myself
- I understand that the school may check my computer files and may monitor the internet site I visit
- I will not complete and send forms without permission from my teacher
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission
- I will not open an attachment or download a file unless I have permission or I know and trust the person who has sent it.

**Using e-mail**

- I will ask permission from a teacher before checking e-mail
- I will immediately report any unpleasant messages sent to me because this will help protect other pupils and myself
- I understand that e-mail messages sent to me may be read by others
- The messages I send will be polite and responsible
- I will only e-mail people I know, or who my teacher has approved
- I will only send e-mail when it has been checked by a teacher
- I will never give my full name, my home address or telephone number in an email
- I will never arrange to meet someone I have only ever previously met on the internet or by email or in a chat room, unless my parent or guardian has given me permission and I take a responsible adult with me.
- I know that use of some Social Networking Websites is illegal under national law for children. I will not set up or use a Facebook, Twitter, Snapchat, Google+, Instagram or You Tube account, even if older brothers or sisters or parents say that it is OK, as I know that children under the age of 13 may not uses these sites.

LALEHAM LEA

A Catholic Independent Primary School for boys and girls aged 3 to 11

Headteacher: Mrs. M Reece

# Parent/Pupil E-Safety Agreement Form

Keeping safe: stop, think, before you click!

Pupil name: _____

Class: _____

I have read the school 'rules for responsible ICT use'. My teacher has explained them to me.

I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.

This means I will use the computers, Internet, e-mail, online communities, digital cameras, video recorders, and other ICT in a safe and responsible way. I understand that the school can check my computer files, and the Internet sites I visit and that if they have concerns about my safety, that they may contact my parent / guardian.

I understand that the use of Facebook and YouTube is illegal to children under the age of 13.

Pupil's signature _____

Parent's signature _____

Date: ___/___/___

**Data Protection Statement**

For the purposes of the GDPR Regulations May 2018 (the 'Regulations'), Laleham Lea School is the data controller in relation to all personal information you provide on this form. Laleham Lea School is committed to protecting your privacy and processing such personal information in a manner which meets the requirements of the Regulations. For more information about Laleham Lea's privacy policy please refer to http://www.lalehamlea.co.uk /sites/default/files/policies/Data-Protection-Policy.pdf

**Appendix 3**

## Exemplar Online Safety Incident Log

| **Reporting Log**<br>Group: ..... | | | | | | |
|---|---|---|---|---|---|---|
| Date | Time | Incident | Action Taken | | Incident Reported By | Signature |
| | | | What? | By Whom? | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Appendix 5**

## Filtering and Monitoring Testing

| When the check took place | Who did the check | What they tested or checked | Actions |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

Appendix 6

## Filtering and Monitoring Annual Check

| Task/responsibility | Notes |
|---|---|
| **Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning** | |
| **Responsibility** - DSL and Filtering Provider<br>**Task**- Is your filtering provider a member of the IWF? | Yes (https://www.iwf.org.uk/membership/our-members/) |
| **Responsibility**: DSL and Filtering Provider<br>**Task**: Does your filtering provider use the IWF list? | Yes, we receive regular updates, and these are automatically integrated to all of our customers, regardless of whether they have SurfProtect or just connectivity. |
| **Responsibility**: DSL and Filtering Provider<br>**Task**: Does your filtering provider use the CTIRU list? | Yes, we receive regular updates, and these are automatically integrated to all of our customers, regardless of whether they have SurfProtect or just connectivity. |
| **Responsibility**: DSL and Filtering Provider<br>**Task**: Are you blocking access to adult content? | Yes |
| **Responsibility**: DSL and Filtering Provider<br>**Task**: Is filtering applied to all accounts including guest accounts? (Staff, pupils) | Yes |
| **Responsibility**: DSL and Filtering Provider<br>**Task**: Is filtering applied to all school owned devices? | Yes (unless whitelisting for certain devices has been requested) |
| **Responsibility**: DSL and Filtering Provider<br>**Task**: Is filtering applied to any device which connects to the school broadband connection? | Yes |
| **Responsibility**: DSL and Filtering Provider<br>**Task**: Do you filter all internet feeds including any backup connection? | Yes |
| **Responsibility**: DSL and Filtering Provider<br>**Task**: Is filtering differentiated by age and ability of pupils? | Yes |
| **Responsibility**: DSL and Filtering Provider<br>**Task**: Can filtering handle multilingual content, images, misspellings, abbreviations? | Yes |

| | |
|---|---|
| **Responsibility**: DSL and Filtering Provider<br>**Task**: Can filtering identify VPNs and proxy services and then block them? | Yes - we block VPN connections and proxy services as part of SurfProtect, unless requested not to do so. |
| **Responsibility**: DSL and Filtering Provider<br>**Task**: Can filtering system provide alerts when access to content has been blocked? | Yes |
| **Responsibility**: DSL and Filtering Provider<br>**Task**: Does filtering work on mobile devices?<br>Is there evidence, have you checked? | Yes |
| **Responsibility**: DSL and Filtering Provider<br>**Task**: Does filtering work on app content?<br>Is there evidence, have you checked? | Yes |
| **Responsibility**: DSL and Filtering Provider<br>**Task**: Will the filtering system identify the IP address, device name and ID and where possible the individual who has attempted to access unsuitable or illegal content? | Yes, we do not use device name, but we can filter and log based on the authenticated username, Internal or external IP |

- Compliant with the DfE Prevent duty standard.
- Compliant with the DfE filtering guidelines.
- KCSiE compliant.
- Utilise PDNS service, enhancing cyber resilience.
- Access to Exa Foundation – Training and Lessons for Parents, Pupils and Staff (https://exa.net.uk/foundation/foundation-about-us/)
- Regularly improving the service to ensure any new DfE recommendations and requirements are met. For example, the network supports the Policy Cyber Alarm and EXA also offer this as a hosted service.
- Excellent customer service – one direct phone number with only two departments. Direct technical support accepted form the end user as well as via Virtual IT.
- Lines are provided on best carrier available for the customers location (BT, Virgin, City Fibre, TalkTalk etc).
- 99.9% uptime.
- ISPA multi award winner.
- Cyber Essentials certified.

All Exa filtering products: The default categories that are blocked are as follows:

| | | |
|---|---|---|
| Adult / Sexually Explicit | Forums or Blogs | Spyware |
| Illegal Drugs | Gambling | Streaming Media |

| | | |
|---|---|---|
| Intimate Apparel / Swimwear | Hacking | Suicide & Self harm |
| Intolerance & Hate | Illegal Filesharing | Tasteless & Offensive |
| Proxies / Translators | Peer to Peer | Virus Worm Infected |
| Violence | Personals & Dating | |
| Weapons | Phishing / Online Fraud | |
| Advertisements or Pop-Ups | Photo Searches | |
| Alcohol & Tobacco | Ringtones / Mobile Downloads | |
| Chat | Social Networking | |
| Criminal Activity | Spam URLs | |