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	January 2026	*M Reece* Headteacher
Ratified by the Board of Governors	January 2026	Y Epale Chair of Governors
Date of next review	January 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 todays 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 al 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, 2025;
- 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 (PSHEE) 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.

- Whilst 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.
- The digital and technology standards in schools' guidance states that the governing body should identify and assign a member of the leadership team and a governor to be responsible for ensuring these standards are met.
- We recognise that all members of the community have important roles and responsibilities to play with regards to online safety.

Governors

The Governors are responsible for the approval of the Online Safety Policy and reviewing the effectiveness of it regularly. Regular meetings and information will be provided to the Governors so they are able to make the correct recommendations; they will also be able to carry out regular monitoring of Online Safety incident logs when required.

The Governors are responsible for ensuring their school has appropriate filtering and monitoring systems in place and regularly review their effectiveness.

Headteacher and Senior Leadership Team

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.

- Ensure that online safety is a running and interrelated theme whilst devising and implementing the whole school approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies (including the staff code of conduct and/or acceptable use policies) and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.

- Ensure that they are doing all that they reasonably can to limit children's exposures to risks from the school's IT system and therefore have appropriate filtering and monitoring systems in place. They will have an awareness and understanding of the provisions in place and will work with technical staff to monitor the safety and security of our systems and networks.

- Ensure that all relevant staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively as well as knowing how to escalate concerns when identified.

- Ensure that they regularly review the effectiveness of filters and monitoring systems; as schools increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material (including when they are online at home).

- Ensure that the DfE's filtering and monitoring standards for schools and colleges are being met; this will be supported through using the checklist appended to this policy and making use of the government resource Plan technology for your school.

- Make use of the government guidance Generative AI: product safety expectations to ensure the safe use of generative artificial intelligence within schools.

- Ensure that online safety is embedded within a progressive preventative curriculum, which enables all learners to develop an age-appropriate understanding of online safety.

- Ensure that ALL members of staff receive regular, updated, and appropriate online safety training which is integrated, aligned and considered as part of the whole school safeguarding approach and know how to escalate concerns when identified.

- Support the DSL and deputies by ensuring they have the additional time, funding, training, resources and support they need to carry out the role effectively.

- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.

- Audit and evaluate online safety practice, annually and as part of this review process, to identify strengths and areas for improvement.

- Communicate with parents regarding the importance of children being safe online, the systems being used in school and information regarding what their children are being asked to do online by the school.

Online Safety Lead (also the schools Designated Safeguarding Lead)

- Be an appropriate senior member of staff from the school leadership team.
- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the schools' safeguarding responsibilities and that a coordinated approach is implemented.
- Liaise with staff (especially teachers, pastoral support staff, SENCOs and the outsourced IT support company) on matters of safeguarding that include online and digital safety.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety, including filtering and monitoring and have the relevant knowledge and up to date training required to keep learners safe online
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns to the Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually).
- Meet regularly with the governor with a lead responsibility for safeguarding and online safety.

Technical Staff

The Network Manager /ICT Technician is responsible for ensuring:

- They provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures and compliance with DfE's filtering and monitoring standards for schools and colleges.
- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That users may only access the school's networks through properly enforced password protection, in which passwords are regularly changed.
- That he/ she keeps up to date with relevant Online Safety technical information and guidance in order to carry out the role effectively.
- That monitoring software/ systems are implemented and up dated regularly.
- Report any filtering breaches to the DSL (or deputy DSLs) and SLT, as well as, the schools Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL (or deputy DSLs), in accordance with the safeguarding procedures.

Teaching and Support Staff

- Be aware that technology is a significant component of many safeguarding and wellbeing issues and that children are at risk of abuse online as well as face to face and that in many cases abuse will take place concurrently via online channels and in daily life.
- Contribute to the development of online safety policies.
- Read and adhere to the Online Safety Policy and Acceptable Use Policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the schools' safeguarding policies and procedures.
- Proactively monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and consistently implement current policies with regard to these devices
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

- Ensure that students are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Reinforce the school's online safety messages when teaching lessons online
- In lessons where internet use is pre-planned, students/pupils should be guided to sites checked as suitable for their use and that any unsuitable material that is found in internet searches is reported for blacklisting.

Pupils

Pupils and students are responsible for-

- Engage in age-appropriate online safety education opportunities provided by the school.
- Using the school digital technology systems in accordance with the student/pupil acceptable use policy.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult or other support services, if there is a concern online, and support others that may be experiencing online safety issues.
- Knowing the policy on mobile phones, digital cameras and other handheld devices and to realise these can be used for cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Laleham Lea's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/ Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Schools should take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local online safety campaigns/literature. Parents and carers should be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

Parents and carers have the responsibility to ensure that their children use the internet and mobile phones correctly and do not misuse these technologies. They should seek help and support from the

school, or other appropriate agencies, if they or their child encounter risk or concerns online. They must be aware of the schools Acceptable Use Policy and agree to it (Appendix 2).

4. Education

Pupils -

All pupils will receive planned Online Safety lessons throughout ICT/ P.S.H.E lessons. These lessons will be regularly revisited and revised to suit the new technologies in and out of school. Key messages will be delivered through a variety of assemblies to ensure all children are aware of the matter. They will also be made aware to question the validity of information which they find online. The school will take part in high profile events/campaigns e.g., Safer Internet Day.

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages in the use of ICT across the curriculum.

In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit at all times.

Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.

We recognise that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL), EYFS (Early Years Foundation Stage) children and children experiencing trauma or loss.

We recognise that children with cognitive difficulties may be unable to understand the difference between fact and fiction in online content and then may repeat the content/behaviours without understanding the consequences of doing so.

We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.

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.org.uk, www.saferinternet.org.uk/
- http://www.childnet.com/parents-and-carers,
- National Online Safety (NOS) Parent APP.

Staff-

All staff must understand the inherent dangers of the online world and be prepared to support and guide our pupils. All new staff will receive Online Safety training as part of the induction process, ensuring they are fully aware and understand the Online Safety policy and the Acceptable Use Policy. The Online Safety Lead will attend regular updates provided by the Local Authority or other training schemes and report back to staff any new issues that they need to be aware of. The Online Safety Lead will provide guidance for any member of staff that seeks it.

Formal annual training including:

- policy updates.
- coverage of the reporting/monitoring systems and staff responsibilities.
- coverage of appendix 1: IT Acceptable Use Policy
- staff sign the agreement on joining the school.
- coverage of the staff code of conduct in relation to online activity/acceptable use and the expectation that staff act as role models.
- best practice for safe usage during lessons, e.g., visible usage and pre-checked internet sites/content.
- use of TES develop.

Staff will be aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.

Staff will be aware that their online conduct outside of the school, including personal use of social media, could have an impact on their professional role and reputation.

All members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

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 reaching 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:

o Use strong passwords for access into our system.
o Use a separate password for your work and personal accounts.
o Always keep their password private; users must not share it with others or leave it where others can find it.
o Not to login as another user at any time.
o Use two-factor/two-step verification for all accounts which have access to personal or sensitive operational data and functions.
o 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. <u>Technical Security Procedures</u>

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 has significant benefits within the curriculum and enhances learning. Image and videos can either be taken by staff and pupils for educational purposes or downloaded from the internet to support learning in the classroom. However, staff and pupils need to be aware of the risks associated with sharing images, especially via the internet. Staff and pupils need to be aware that once an image/ video is posted on the internet that it will remain there forever. This could cause harm or embarrassment in the future.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites.

Staff are allowed to take digital / video images to support educational purposes, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

Care should be taken that when capturing images/ videos that all pupils concerned are appropriately dressed and not participating in activities that could bring either the pupils or the school into disrepute.

Pupils' full names will not be used anywhere on the website or in blogs and particularly not associated with photographs there.

Written permission must be obtained from the parent or carer of any child before pictures are published on the website. Written permission is provided for every child that starts the school to indicate whether the parent or carer allows their child to be photographed.

Laleham Lea School will always comply with the Data Protection Act 2018 in regards to digital images and videos.

8. **Mobile Phones**

We recognise that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within the school.

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

- Members of staff are allowed to bring their personal mobile device into school. However, they are required to use their devices only in the designated areas authorised by the SLT, or in an area where no children are present.
- We have signs around our school indicating that we are a mobile phone free site. Our staff support and fully understand.
- Staff will be advised to:
  - Keep mobile phones and personal devices in a safe and secure place (bags) during lesson time.

- o Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
- o Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled when in the school.
- o Not use personal devices during teaching periods, unless permission has been given by the headteacher such as in emergency circumstances

- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
- Staff will not use personal devices to take photos or videos of learners and will only use work-provided equipment for this purpose.

If a member of staff breaches our policy, action will be taken in line with our Code of Conduct/Staff Behaviour and Allegations Policy

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

Learners' Use of Personal Devices and Mobile Phones
- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Laleham Lea School does not allow pupils to bring electronic devices into School, this includes Smart watches (meaning that they would not be able to access 3G/4G/5G services).
- In exceptional circumstances this may be necessary e.g., for medical reasons, and these will be kept in the office.
- Pupils are not permitted to bring any mobile or electronic devices with imaging and sharing capabilities, including Smart watches or cameras on school trips, instead, staff members take pictures of the children using school cameras during outings/residential trips and these images are then shared with parents after the trip.

Visitors' Use of Personal Devices and Mobile Phones
- Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, safeguarding and child protection and mobile phone and photographic.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.

- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputies) or headteacher of any breaches of our policy.

9. Unsuitable Use, Sanctions and Reporting

It is expected that all users will be responsible and safe users of ICT, who understand the policy and work within it. However, at times an infringement of the policy may occur whether through carelessness or, very rarely, deliberately.

Illegal or inappropriate activity

The school believes that the activities listed below are inappropriate in a school context (those in bold are illegal) and that users should not engage in these activities when using school equipment or systems (in or out of school). Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- **child sexual abuse images** (illegal - The Protection of Children Act 1978);
- **grooming, incitement, arrangement or facilitation of sexual acts against children** (illegal–Sexual Offences Act 2003);
- **possession of extreme pornographic** (illegal–Criminal Justice and Immigration Act 2008);
- **criminally racist material in UK criminally racist material in UK–to stir up religious hatred (or hatred on the grounds of sexual on the grounds of sexual orientation)** (illegal– Public Order Act 1986);
- democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs (Prevent Strategy 2011 – See SMSC policy);
- pornography;
- promotion of any kind of discrimination;
- promotion of racial or religious hatred;
- threatening behaviour, including promotion of physical violence or mental harm; or
- any other information that may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.

Additional Inappropriate Activity
It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal disciplinary procedures. The following is also considered to inappropriate activity at Laleham Lea School:

- using school systems to run a private business;
- use systems, applications, websites, or other mechanisms that bypass the filtering or other safeguards employed by the school (i.e., proxy services);
- uploading, downloading, or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions;
- revealing or publicising confidential or proprietary information (e.g., financial or personal information, databases, computer or network access codes and passwords);
- creating or propagating computer viruses or other harmful files;
- carrying out sustained or instantaneous high volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the internet;
- online gambling and non-educational gaming;
- use of personal social networking sites and profiles for non-educational purposes.

The correct reporting procedure is in place and all staff are aware of who to speak to in the first instance. Appendix 3 shows the Online Safety Incident Log which needs to be completed in this instance. This being, speaking to the Online Safety Lead, who will then investigate the matter. If the matter is of a serious nature, then either the Designated Safeguarding Lead or the Headteacher will be informed, who will take the matter further.

All children will be made aware of the importance to report any incident to either an adult at school that they can trust or the 'Report Abuse' button that is present on the school website, regarding any incidents that may occur outside of school.

If an incident has occurred due to carelessness, this will to be investigated and the correct sanctions will be implemented. All users within the school are aware that there is a monitoring system that is in place and is sensitive enough to pick up slight infringements regarding; cyber-bullying, searching for inappropriate content etc.

In all cases the Headteacher when notified will decide what action to take and whether the incident needs further action, e.g., reporting to police, Local Authority.

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.

Laleham Lea Primary School, 29 Peaks Hill, Purley, Surrey, CR8 3JJ

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 Primary School, 29 Peaks Hill, Purley, Surrey, CR8 3JJ

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

Laleham Lea Primary School, 29 Peaks Hill, Purley, Surrey, CR8 3JJ

Appendix 3

Exemplar Online Safety Incident Log

Reporting Log Group:						
Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Laleham Lea Primary School, 29 Peaks Hill, Purley, Surrey, CR8 3JJ

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 **Task**- Is your filtering provider a member of the IWF?	Yes (https://www.iwf.org.uk/membership/our-members/)
Responsibility: DSL and Filtering Provider **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 **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 **Task**: Are you blocking access to adult content?	Yes
Responsibility: DSL and Filtering Provider **Task**: Is filtering applied to all accounts including guest accounts? (Staff, pupils)	Yes
Responsibility: DSL and Filtering Provider **Task**: Is filtering applied to all school owned devices?	Yes (unless whitelisting for certain devices has been requested)
Responsibility: DSL and Filtering Provider **Task**: Is filtering applied to any device which connects to the school broadband connection?	Yes
Responsibility: DSL and Filtering Provider **Task**: Do you filter all internet feeds including any backup connection?	Yes
Responsibility: DSL and Filtering Provider **Task**: Is filtering differentiated by age and ability of pupils?	Yes
Responsibility: DSL and Filtering Provider **Task**: Can filtering handle multilingual content, images, misspellings, abbreviations?	Yes

Responsibility: DSL and Filtering Provider **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 **Task**: Can filtering system provide alerts when access to content has been blocked?	Yes
Responsibility: DSL and Filtering Provider **Task**: Does filtering work on mobile devices? Is there evidence, have you checked?	Yes
Responsibility: DSL and Filtering Provider **Task**: Does filtering work on app content? Is there evidence, have you checked?	Yes
Responsibility: DSL and Filtering Provider **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.
- Utilize 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	