Littledean Church of E Primary School and Pre-School

Online Safety Policy

Littledean C of E Primary School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

Content	Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm, suicide, and discriminatory or extremist views.
Contact	Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit them.
Conduct	Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
Commerce	Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Legal Framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2023) 'Keeping children safe in education 2023'
- DfE (2023) ' Teaching online safety in schools'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 20202 edition'
- National Cyber Security Centre (2020) 'Small business guide: cyber security'

Roles and Responsibilities

The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of the filtering and monitoring systems is reviewed at least annually in liaison with IT staff and service providers.

- Ensuring the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Head Teacher will be responsible for:
- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and DDSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL/DDSL and IT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an annual basis.

The DSL (who is also the Head Teacher) will be responsible for:
- Taking the lead responsibility for online safety on school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENDCO and IT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems in the school.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a termly basis.

All staff members will be responsible for:
- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online,
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns.

Managing Online Safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly due to the rise of social media

The following measures have been adopted to help ensure that our children are not exposed to unsuitable material:

- Our internet access provides a service designed for children in a school setting, including a 'firewall' filtering system through SWGFL; intended to prevent access to material inappropriate for children.
- Children using the internet will normally be working in the classroom during lesson time and supervised by an adult. If children use the internet during lunchtimes, to plan collective worship for example, this will also be supervised by an adult.
- Staff will check that the sites pre-selected for the children to use are appropriate to the age and maturity of the children.
- If staff discover an unsuitable site, it will be reported to the class teacher and then to the School Business Manager who will inform our IT support technician who will subsequently ensure that the site is blocked. SWGFL will also be informed.
- Children will be taught to use e-mail and the internet responsibly in order to reduce the risk to themselves and others.
- Children will have access to information from relevant outside agencies.
- Children using the school's computing facilities will be expected to comply with the above measures.

The Curriculum

The children are taught computing skills in line with the objectives outlined in the National Curriculum and through our scheme TEACH Computing. In order to specifically teach skills related to online safety, as well as drip feeding online safety strategies throughout the year, children also complete a whole unit of work on online safety each year, building up skills and knowledge at an age appropriate level. The school have also employed the SCARF PSHE teaching and learning scheme which also covers online safety in the 'Keeping Safe' units of work.

Reception	• Show resilience and perseverance in the face of a challenge. • Know and talk about the different factors that support their overall healthand wellbeing: • Develop an understanding of sensible amounts of 'screen time'.
Year 1	• Create, name and date digital creative work. • Safely search for images online. • Understand how to communicate safely online. • Understand what personal information needs to be kept safe. • Explore how to use email to safely communicate. • Apply online safety knowledge to help others make good choices online.
Year 2	• Understand that the information put online leaves a digital footprint. • Use keywords in an online search to find out about a topic. • Recognise whether a website is appropriate for children. • Rate and review informative websites. • Identify kind and unkind behaviour online. • Apply knowledge of safe and sensible online behaviours to different situations.
Year 3	• Know what cyberbullying is and how to address it. • Understand how websites use advertisements to promote products. • Create strong passwords and understand privacy settings. • Safely send and receive emails. • Explore different ways children can communicate online. • Use knowledge about online safety to plan a party online.
Year 4	• Know how a message can hurt someone's feelings. • Say how to respond to hurtful messages online. • Use a search engine correctly. • Understand the term 'plagiarism' and how to avoid it. • Create a safe online profile. • Explain how to be a responsible digital citizen. • Create an online safety superhero character.

Year 5	• Identify spam emails and know what to do with them. • Write citations for the websites that are used for research. • Create strong passwords. • Recognise when, how and why photographs seen online might have been edited. • Apply online safety rules to real-life scenarios.
Year 6	• Find similarities and differences between in-person and cyberbullying. • Identify good strategies for dealing with cyberbullying. • Identify secure websites by identifying privacy seals of approval. • Understand the benefits and pitfalls of online relationships. • Identify information that should never be shared. • Identify how the media play a powerful role in shaping ideas about gender. • Apply online safety knowledge to the creation of a quiz.

Handling Online Safety Concerns

Any disclosures made by children to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Safeguarding and Child Protection Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that children displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and any information may still be shared lawfully, for example if the DSL decides that there is a legal basis under UK GDPR such as the public tasks basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reason for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the Head Teacher, who decides on the best course of action in line with relevant policies. If the concern is about the Head Teacher, it is reported to the Chair of Governors.

Concerns regarding a child's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Head Teacher, Mental Health Lead, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Regulation Policy and the Safeguarding and Child Protection Policy.

Where there is a concern that illegal activity has taken place, the Head Teacher contacts the police.

The school avoids unnecessarily criminalising children, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Safeguarding and Child Protection Policy.

All online safety incidents will be recorded on My Concern.

Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or some else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g Facebook
- Abuse between young people in intimate relationships online, e.g. teenage relationship abuse
- Discriminatory bullying online, e.g. homophobia, racism, misogyny/misandry

The school will be aware that certain children can be more at risk of abuse and/or online bullying, such as LGBTQ+ and children with SEND.

Cyberbullying against children or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively.

Child on Child Sexual Abuse and Harassment
Children may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff understand that this abuse can occur both in and outside of school, off line and online, and will remain aware that children are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviours of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, e.g. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual taunts or jokes
- Unwanted and unsolicited sexual comments and messages
- Consensual and non-consensual sharing or sexual imagery
- Abuse between young people in intimate relationships online, e.g. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to children becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, e.g. individuals under the age of 18, is a criminal offence, even when the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social following the initial report, as well as interactions with other children taking 'sides', often leading to repeat harassment.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on school grounds or using school owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL/Head Teacher, who will investigate the matter in line with the Safeguarding and Child Protection Policy.

Grooming and Exploitation
Grooming is defined as the situation whereby an adults builds a relationship, trust and emotional connections with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that children who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the child may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact that children are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. Signs of online grooming include:

- Being secretive about how they are spending their time online
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain

Child Sexual Exploitation (CSE) and Child Criminal Exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a child may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have concerns about children in regards to CSC or CCE, they will bring these to the DSL without hesitation, who will manage the situation in line with the Safeguarding and Child Protection Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making then more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain children at increases vulnerability to radicalisation. Staff will be expected to exercise vigilance towards any children displaying indicators that they have been, or are being, radicalised.

Where staff have concerns about children in regards to radicalisation, they will bring these to the DSL without hesitation, who will manage the situation in line with the Safeguarding and Child Protection Policy.

Mental Health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a child's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a child is suffering from challenged in their mental health.

Online Hoaxes and Harmful Online Challenges

For the purposes of this policy, an 'online hoax' is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, 'harmful online challenges' refers to challenged that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video

through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the child and the way in which they are depicted in the video.

Where staff suspect there may be harmful online challenges or online hoaxes circulating amongst children in the school, they will report this to the DSL immediately.

The DSL/Head Teacher will conduct a case-by-case assessment for ant harmful online content brought to their attention, establishing the scale and nature of the possible risk to children, and whether the risk is one that is localised to the school or local areas, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL/Head Teacher will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL/Head Teacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact checking the risk of online challenges or hoaxes.
- Careful to avoid needless scaring or distressing children.
- Not inadvertently encouraging children to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger children but is almost exclusively being shared amongst older children.
- Proportional to the actual or perceived risk.
- Helpful to children who are, or perceived to be, at risk.
- Appropriate for the relevant children's age and developmental stage.
- Supportive.
- In line with the Safeguarding and Child Protection Policy.

Where the DSL/Head Teacher's assessment finds an online challenge to be putting children at risk of harm, they will ensure that the challenge is directly addressed to the relevant children, e.g. those within a particular age range that is directly affected or individual children at risk where appropriate.

The Head Teacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing children's exposure to the risk is considered and mitigated as far as possible.

Cyber-Crime

Cyber-crim is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and be conducted at higher scales and speed online, e.g. fraud, purchasing and selling of illegal drugs and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting' which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that children with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are concerns about a child's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

Online Safety Training for all Staff

The DSL/Head Teacher will ensure that safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and

responsibilities relating to filtering and monitoring systems. All staff will be made aware that children are at risk of abuse, by their peers and by adults, online as well as in person, and that often abuse will take place concurrently via online channels and in daily life.

Use of Technology in the Classroom
A wide range of technology will be used during lessons, including the following:

- Laptops
- I-pads
- Cameras
- Bee-bots
- Email

Prior to using ant websites, tools, apps or other online platforms in the classroom, or recommending that children use them at home, the class teacher will review and evaluate the resource. Children will be supervised when using online materials during lesson times.

Educating Parents
The school will work in partnership with parents to ensure children stay safe inline at school and at home. Parents will be provided with information about the school's approach to online safety through access to our curriculum documents on the school website and also signposting information for parents also available on the school website.

Filtering and Monitoring Online Activity
The Governing Board will ensure that the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and Monitoring Standards for Schools and Colleges'. The Governing Board will ensure 'over blocking' does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

The DSL/Head Teacher will ensure that specific roles and responsibilities are identified and assigned to manage the filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The filtering and monitoring systems that school implements will be appropriate to the children's ages, the number of children using the network, how often children access the network and the proportionality of costs compared to the risks. IT technicians will undertake a monthly check on filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the Head Teacher. Prior to making any changes to the filtering system, IT technicians and the Head Teacher will conduct a risk assessment. Any changes made to the system will be recorded by the Head Teacher. Reports of inappropriate websites or materials will be made to the Head Teacher and UT technicians immediately and the matter will be investigated and any necessary changes made.

Deliberate breaches of the filtering system will be reported to the Head Teacher. If a child has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Regulation Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

Internet Access
Technical security features, such as anti-virus software, will be kept up-to-date and managed by IT technicians. Firewalls will be switched on at all times. Staff and children will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to the IT Technicians.

All members of staff will have their own unique username and password to access the school network. Users will inform the IT Technicians if they forget their log in details.

Emails
Staff will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Monitoring and Review
The school recognises that the online world is constantly changing; therefore, this policy will be reviewed annually.

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff
- Acceptable Use
- Safeguarding and Child Protection
- Anti-Bullying and Hate
- Staff Handbook
- Behaviour Regulation
- Disciplinary Policy and Procedure
- Data Protection
- Confidentiality

Date of Review: November 2023
Date of Next Review: November 2026