Online Safety Policy

October 2025 – October 2028

Christian Vision

Building strong foundations for a happy and successful life

Like the wise man who built his house on rock (Matthew 7: 24-27), we seek God's wisdom to enable us to nurture our school community so that all can flourish and achieve their best in every aspect of school life.

Online Safety Intent

Computing and the use of digital devices are seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. The rapid development in electronic communications is having many effects on society. At this present time, every child in school has access to the internet at school and the majority go on-line at home. Whilst exciting and beneficial, all users need to be aware of the range of risks associated with the use of these technologies.

At Lewknor Church of England Primary, we understand the responsibility to educate our pupils on online safety. Online safety encompasses internet technologies and electronic communications. We endeavour to highlight the benefits and risks of using technology and teach the pupils how to safeguard themselves online. The school's online safety policy will operate in conjunction with other school policies and procedures. It will also be based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

Internet use is part of the statutory curriculum and is a necessary tool for staff and pupils. The school has a duty to provide students with quality internet access as part of their learning experience. Pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents and carers.

Implementation

It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues.

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in our school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

• We will provide a curriculum/Jigsaw curriculum/computing curriculum and other lessons which have online safety lessons embedded throughout.

• We will celebrate and promote online safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.

• We will discuss, remind or raise relevant online safety messages with pupils routinely, wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital material.

• Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objective for a specific curriculum area.

• Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.

• We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.

• When searching the internet for information, pupils will be guided to use age appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.

• Pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying (see Anti-Bullying Policy).

• Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member.

Remote Teaching

• We will endeavour to ensure that pupils continue to receive a good level of education 'beyond the classroom' by providing a range of resources via our website and through Microsoft Teams.

• We expect pupils to follow the same principles, as outlined in the school's Acceptable Use policy, whilst learning at home.

• If our school chooses to communicate with pupils via Teams etc. pupils must uphold the same level of behavioural expectations, as they would in a normal classroom setting.

• Any significant behavioural issues occurring on any virtual platform must be recorded and reported to the Headteacher and appropriate sanction imposed. For all minor behavioural incidents, these should be addressed using the normal restorative approaches.

• Staff should be mindful that when dealing with any behavioural incidents which occur online, opportunities to discuss and repair harm will not be the same as if the child or young person was in school. Therefore, it may be necessary to have a discussion with the parents, regardless how minor the incident, to ensure the child is emotionally well supported.

• All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

• All staff will be encouraged to incorporate online safety activities and awareness within their curriculum areas.

Roles and Responsibilities

Governing Body

The Governing Body is accountable for ensuring that Lewknor Primary School has effective policies and procedures in place.

Headteacher

Reporting to the Governing Body, the Headteacher has overall responsibility for online safety within our school. The day-to-day management of this will be delegated to a member of staff, the Online Safety Lead, as indicated below .

The Headteacher will ensure that:

- Online safety training throughout the school is planned and up-to-date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team and governing body, parents.

- The designated Online Safety Lead has had appropriate training in order to undertake the day-to-day duties.

- All Online Safety incidents are dealt with promptly and appropriately.

Online Safety Lead

The Online Safety Lead will:

- Keep up-to-date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.

- Review this policy regularly and bring any matters to the attention of the Headteacher.

- Advise the Headteacher and governing body on all online safety matters.

- Engage with parents and the school community on online safety matters at school and/or at home.

- Liaise with the local authority, IT technical support and other agencies as required.

- Retain responsibility for the online safety log; ensure staff know what to report and ensure the appropriate audit trail.

- Ensure any technical online safety measures in the school (e.g. internet filtering software, behaviour management software) are fit for purpose through liaison with the school's Technical Support.

- Make themselves aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Lead immediately.

- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the Online Safety Lead and Headteacher.

- If users discover a website with potentially illegal content, this should be reported immediately to the Online Safety Lead. The school will report such incidents to appropriate agencies including Internet Service Provider (ISP), Police, or the Internet Watch Foundation (IWF).

- Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.

All Staff

Staff are to ensure that:

• All details within this policy are understood. If anything is not understood, it should be brought to the attention of the Headteacher or the Online Safety Lead.

• Any online safety incident is reported to the Online Safety Lead (and incidents are recorded), or in their absence to the Headteacher. If you are unsure, the matter is to be raised with the Online Safety Lead or the Headteacher to make a decision.

All Pupils

The boundaries of use of equipment and services are given in the Pupil Acceptable Use Policy; any deviation or misuse of equipment or services will be dealt with in accordance with the Behaviour Policy.

• Online safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly, all pupils will be fully aware how they can report areas of concern whilst at school or outside of school.

• Pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying. See Anti-Bullying Policy.

• Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member.

Parents and Carers

Parents and carers play the most important role in the development of their children; as such Lewknor Primary School will ensure that opportunities are made to support parents so that they have the skills and knowledge they need to ensure the safety of children outside the school environment. Through assemblies, social media, the school website and other events in school, the school will keep parents up to date with new and emerging online safety risks, and will involve parents in strategies to ensure that pupils are empowered.

Parents must also understand that Lewknor Primary School needs to have rules in place to ensure that their child can be properly safeguarded. As such, parents will sign the Pupil Acceptable Use Policy before any access can be granted to school equipment or services.

Technology

Lewknor Primary School uses a range of devices including PCs, laptops and iPads. In order to safeguard the pupils and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering

This software prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites (appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner). The Computing Lead, Online Safety Lead and external technical support staff (Turn It On) are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher. The filtering will be reviewed regularly. Virus protection will also be installed and updated regularly. Personal data sent over the internet will be encrypted or otherwise secured. Files held on the school's network will be regularly checked.

Personal Data

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. Lewknor Church of England Primary School aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. Refer to Lewknor Church of England Primary School's 'Data Protection Policy'.

Passwords

All staff and pupils will be unable to access any device without a unique username (passwords for staff). Staff passwords will be changed if there has been a compromise.

Anti-Virus

All capable devices will have anti-virus software. This software will be updated regularly for new virus definitions. IT Support will be responsible for ensuring this task is carried out and will report to the Headteacher if there are any concerns.

Mobile Phones

No pupil should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be locked away until the end of the day.

Mobile phones and personally-owned devices that belong to members of staff or visitors in the school will not be used in any areas where children will be during school hours.

Safe Use

Internet

Use of the internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing the Staff Acceptable Use Policy and to pupils upon signing and returning their acceptance of the Pupil Acceptable Use Policy.

Email

All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work based emails only. Staff should not use personal email accounts for professional purposes, especially to exchange any school related information or documents or to email parents/carers. Emails of a personal nature are not permitted. Similarly, use of personal email addresses for work purposes is not permitted. The secure email system (EDT) should be used at all times to send sensitive data outside the school system.

When the pupils use our approved email accounts on the school system, pupils:

- May only use approved email accounts on the school system
- Must immediately tell a teacher if they receive offensive messages
- Must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission
- Must not access others pupil's accounts or files
- Must be responsible for their own behaviour on the internet, just as they are anywhere else in the school. This includes the materials they choose to access, and the language they use
- Must not deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the school can block further access to the site
- Are expected not to use any rude or offensive language in their email communications, and contact only people they know or those the teacher has approved. They will be taught the rules of etiquette for email and will be expected to follow them
- Must understand the forwarding of chain letters is not permitted

Media & Networking Social

There are many social networking services available. Lewknor Primary School is fully supportive of social networking as a tool to engage and collaborate with parents, carers and the wider school community. The following social media services are permitted for use within the school and have been appropriately risk assessed; should staff wish to use other social media; permission must first be sought via the Online Safety Lead who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

• Facebook – used by the staff in school as a broadcast service. No persons will be 'followed' or 'friended' on these services and as such no two-way communication will take place. In addition, the following is to be strictly adhered to:

• Permission for photographs and videos to be used on social media, websites and around school will be sought from parents when children join our school, and updated if anything changes. This information will be collected and all members of staff will be made aware of who and who cannot be photographed/ videoed.

• There is to be no identification of any pupil using first name and surname; first name only is to be used.

• Where services are 'comment enabled', comments are to be set to 'moderated'.

• All posted data must conform to copyright law; videos and other resources that are not originated by Lewknor Primary School are not allowed unless the owner's permission has been granted or there is a licence which allows for such use.

• Staff will not post inappropriate content or participate in any conversations which will be damaging or be deemed detrimental to the image of the school.

• Members of staff who hold a personal account should not have pupils (past or present) as their 'friends' or 'followers' on social media. Staff should also not have any parents or as their 'friends'/ 'followers', unless the 'relationship' with the parent pre-exists before child starts school.

For Pupils at Lewknor C of E Primary they are not allowed to access social networking sites in school and if they access these sites at home, they are advised to:

• Never give out personal details of any kind which may identify them or their location

• Not to place personal photos on any social network space

• Think about their security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications

• Only accept invitations of known friends and deny access to unknown people

Pupils and parents are made aware that some social networks are not appropriate for children of primary school age and that there is a legal age to hold accounts on many social media sites. The school will work in partnership with our technical support team to ensure filtering systems are as effective as possible and children are unable to access social media sites on their pupil login.

Photos and Videos

Working with children and young people may involve the taking or recording of images. Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and wellbeing of children and young people. Informed written consent from parents or carers and agreement, where possible, from the child or young person, should always be sought before an image is taken for any purpose.

Dojo

ClassDojo is a school communication platform that teachers and families use every day to develop parental partnerships between school and home and it is also used as part of our Positive Behaviour Policy. Teachers and parents can send messages to each other via ClassDojo regarding pupils, what they have been learning in

the classroom and any achievements. In the event of remote learning taking place, parents are encouraged to send in photographs of their child's work so that teachers can support and celebrate achievements. Communication with parents should only take place on ClassDojo during the hours of 8am - 6pm and conversations should be professional.

Incidents

Any online safety incident should be brought to the immediate attention of the Online Safety Lead, or in their absence the Headteacher. The Online Safety Lead will assist in taking the appropriate action to deal with the incident. Incidents will be documented and actions will be taken by appropriate members of staff. An important element of online safety is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff/volunteers, children and young people have a responsibility to report online safety incidents promptly so that they may be dealt with effectively. The school has incident reporting procedures in place and know how to records incidents.

Online sexual harassment

Sexual harassment is likely to: violate a child's dignity, make them feel intimated, degraded or humiliated and/or create a hostile, offensive or sexualised environment. Online sexual harassment, which might include: non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats). Any reports of online sexual harassment will be taken seriously, and the police and Children's Social Care may be notified. Our school follows and adheres to the national guidance - UKCCIS: Sexting in schools and colleges: Responding to incidents and safeguarding young people, 2016.

Lewknor Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RE curriculum.

If content is contained on learner's electronic devices, they will be managed in accordance with the DfE **'searching screening and confiscation'** advice.

The Education Act 2011, allows staff to lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

• cause harm;

• disrupt teaching;

• break school rules;

• commit an offence;

• cause personal injury;

• damage property.

Radicalisation Procedures and Monitoring

It is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via Safeguarding Lead). Regular monitoring and filtering is in place to ensure that access to inappropriate material on the internet and key word reporting is in place to ensure safety for all staff and pupils.

Complaints

Complaints of internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Headteacher. Parents and pupils will need to work in partnership with staff to resolve issues. Sanctions within the school discipline policy include:

o Interview/counselling by the Headteacher

o Informing parents or carers

o Removal of internet or computer access for a period of time.

Impact

The curriculum of online safety has been created to ensure that children have as much knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. We want to ensure online safety is meaningful and memorable so children can always relate back to their learning if they ever found themselves in a situation online.