Lewknor Church of England Primary School
E-Safety Policy
November 2019 - review November 2022

Internet Use

The rapid development in electronic communications is having many effects on society. The internet is an essential element in 21st century life for education, business and social interaction. At this present time, every child in school has access to the internet at school and the majority go on-line at home. Many use it more often and with more expertise than adults. At Lewknor Primary School, we believe that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of the staff and to enhance the school's management information and business administration systems.

Internet use is a 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 takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2018, Early Years and Foundation Stage 2017, and 'Working Together to Safeguard Children' 2018.

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.

Aims

The purpose of Lewknor Primary School E-Safety policy is to:

- Safeguard and protect all members of Lewknor Primary School community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns

How will Internet use enhance learning?

- The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of our pupils
- Children will be taught what internet use is acceptable and what is not and given clear objectives for internet use
- Internet access will be planned to enrich and extend learning activities
- Staff will guide pupils in online activities that will support learning outcomes planned for the pupils' age and maturity
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation

Good Habits

E safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies

- Sound implementation of the E-safety policy, in both administration and curriculum, including secure school network design and use
- Safe and secure broadband from the provider including the effective management of content filtering

Lewknor Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm

Dangers To Consider

Some of the dangers children may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyberbullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. We must demonstrate that we provide the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The E safety policy that follows explains how we intend to do this.

Communication Of E Safety And Internet Usage Policy

Pupils

- Pupils will sign an Acceptable Use Agreement
- Rules for internet access will be posted in all classrooms
- Pupils will be informed that internet use will be monitored
- E-safety will be taught in every classroom to raise the awareness and importance of safe and responsible internet use
- Pupils will be reminded of E safety rules regularly – especially when using the internet

Staff

- All staff will be given a copy of the E safety Policy and its importance explained
- Staff will sign an Acceptable Use Agreement
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues
- Staff training in safe and responsible internet use on the school e-safety policy will be provided as required

Parents

- Parents attention will be drawn to the school's e-safety policy in newsletters and on the school website
- E-safety resources will be linked on the website for parents to access
- Parents acknowledge the content of their child's e-safety agreement by signing the document alongside their child
- Internet issues will be handled sensitively, and parents will be advised accordingly
- A partnership approach with parents will be encouraged. This could include, if necessary, parent evenings or assemblies with demonstrations and suggestions for safe home internet use
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents

Vulnerable Learners

- Lewknor Primary School recognises 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) and children experiencing trauma or loss
- Lewknor Primary School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners. When implementing an appropriate online safety policy and curriculum Lewknor Primary School will seek input from specialist staff as appropriate, including the SENCO

Email & Online Collaboration

- Pupils may only use approved email accounts on the school system
- Pupils must immediately tell a teacher if they receive offensive messages
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission
- Pupils must not access others pupil's accounts or files
- Whole class or group email addresses should be used in school
- Pupils 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
- Pupils 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
- Pupils 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
- Pupils must ask permission before accessing the internet and have a clear idea of why they are using it.
- Computers and school laptops should only be used for school work and homework unless permission has been given otherwise
- No program files may be downloaded from the internet to the computer, to prevent corruption of data and to avoid viruses
- Pupils must not bring in USBs from home for use in school without permission. This is for both legal and security reasons. USBs should be virus scanned before use
- Access in school to external personal email accounts may be blocked
- The forwarding of chain letters is not permitted

Social Networking

- At Lewknor C of E pupils are not allowed to access social networking sites and newsgroups unless a specific use is approved
- Pupils are advised never to give out personal details of any kind which may identify them or their location
- Pupils are advised not to place personal photos on any social network space
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications
- Pupils are encouraged to invite known friends only and deny access to others
- Pupils and parents are made aware that some social networks are not appropriate for children of primary school age and the legal age to hold accounts on many such as YouTube or Instagram is 13 years old
- The school will work in partnership with Internet Service Provider to ensure filtering systems are as effective as possible

Information System Security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly
- Security strategies will be discussed with our technical support team (Turn It On)

Managing systems

- The security of the school information systems will be reviewed regularly by Turn It On who follow OCC guidance
- Virus protection will be updated regularly via the Turn It On and all computers have 'Sophos Anti-Virus' installed
- Security strategies will be discussed with appropriate advisors
- Personal data sent over the internet will be encrypted or otherwise secured
- Personal portable media may not be used without specific permission followed by a virus check
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email
- Files held on the school's network will be regularly checked

Website Monitoring and Safety

- Our website celebrates pupils' work and promotes the school values. The school shares information with other educational professionals
- The website is managed by the School Adminstrator
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs
- Written permission from parents or carers will be obtained before images of pupils are electronically published

Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
- Personal mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden

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'.

Published Content and the School Website

The contact details on the website should be the school's address, email and telephone number. Staff or pupils' personal information will not be published.

The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Risk Assessment

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Surf Protect filtering system provided by Turn It On can accept liability for the material accessed, or any consequences resulting from internet use.
- The school will review the Computing policy on a regular basis to establish if the e-safety policy is adequate and that the implementation of the e-safety is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Monitoring and Review

Technology in this area evolves and changes rapidly. The policy will be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.

- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied
- To ensure they have oversight of online safety, the Head teacher will be informed of online safety concerns, as appropriate
- Any issues identified via monitoring will be incorporated into our action planning

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 head teacher
- Pupils and parents will be informed of the complaints procedure
- Parents and pupils will need to work in partnership with staff to resolve issues
- Sanctions within the school discipline policy include:
    - Interview/counselling by the head teacher
    - Informing parents or carers
    - Removal of internet or computer access for a period of time.

Online Sexual Violence and Sexual Harassment between Children

Our setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2018.

- Lewknor Primary School recognises that sexual violence and sexual harassment between children can take place online. Examples may include: non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
  Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.
- Lewknor Primary School recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Lewknor Primary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- 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.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment we will:
  - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
  - If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
  - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
  - Implement appropriate sanctions in accordance with our behaviour policy.
  - Inform parents and carers, if appropriate, about the incident and how it is being managed.
  - If appropriate, make a referral to partner agencies, such as the MASH and/or Thames Valley Police.
  - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
  - If a criminal offence has been committed, the DSL (or deputy) will discuss this with Thames Valley Police first to ensure that investigations are not compromised.
  - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.