Lewknor Church of England Primary School
E-Safety Policy
September 2016 (Review September 2017)

What is E-Safety?

E-Safety encompasses not only internet technologies but also electronic communications such as smart phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

Principles of E-Safety

- In school, a member of staff who flouts security advice or uses e-mail or the internet for inappropriate reasons risks dismissal.
- All staff sign a code of conduct on appointment. Staff will thereby accept that the school can monitor use of technology to help ensue staff and pupil safety.
- Staff that manage filtering systems or monitor ICT use have great responsibility and must be appropriately supervised. Procedures must define how inappropriate or illegal ICT use is reported to senior management.
- Staff are aware of dangers to themselves in managing ICT use, for instance in viewing inappropriate images.
- Any allegations of inappropriate behaviour must be reported to the head teacher and investigated with great care – an innocent explanation may well exist. E-mail, text messaging and instant messaging all provide additional channels of communication between staff and pupils and inappropriate behaviour can occur, or communications can be misinterpreted.
- Staff might reflect on the power of the technology in police hands to identify the sender of inappropriate messages.
- Children have their own logins which they are given when they begin school so that all children can save their work in their own specific area of the system.

Every Child Matters

E-Safety encompasses all the areas within Every Child Matters.

- Staying safe – Children need to be able to use the internet and school resources safely.
- Being healthy – Children need to be able to learn how to use the internet safely and understand the consequences of inappropriate behaviours. Children need to be supervised to learn about making appropriate choices.
- Enjoying and achieving – Pupils need to be able to use the internet appropriately to support learning. Pupils need to be encouraged to have fun safely using the internet.
- Making a positive contribution – Pupils need to be able to understand how to contribute to e-life in a safe environment.
- Achieving economic wellbeing – Appropriate use of the internet may enhance learning and educational prospects when used appropriately.

Teaching and Learning

Internet use is an essential element of 21st Century learning. The school has a duty to provide quality internet access for their pupils. The purpose of internet use in school is to raise educational standards, to promote pupils' achievement, to support the professional work of staff and to enhance the school's management functions.

Pupils use the internet widely outside school and need to learn how to use it and evaluate internet information and take care of their own safety and security.

Good planning and preparation is critical in ensuring a safe starting point for the development of web search skills and strategies. Tasks can be planned that do not require an internet-wide search engine.

Benefits of using the internet in education include:

- Access to world-wide educational resources;
- Inclusion in the National Education Network which connects all UK schools;
- Educational and cultural exchanges between pupils world-wide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practise;
- Collaboration across support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data within the borough;
- Access to learning wherever and whenever convenient.

Accessing and evaluating information

We use the OCC system for filtering to ensure inappropriate web material is not accessed through school resources. Access to sensitive sites may be required for the duration of a specific educational activity by supervised pupils of appropriate age. OCC filtering software can provide temporary access to specific sites, which a teacher considers necessary for a particular purpose. Clearly pupils need to understand that unselective copying is worth little without a commentary that demonstrates the selectivity used and evaluates significance. Respect for copyright and intellectual property rights, and the correct use of published material should be taught.

- The school will ensure that the copying, and subsequent use, of internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.
- The evaluation of online materials is a part of every subject.

Managing systems

The security of the school information systems will be reviewed regularly by the OCC guidance as they manage the overall system.

- Virus protection will be updated regularly via the OCC network.
- 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.

Email Monitoring

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits and interesting projects between schools in neighbouring villages and in different continents can be created. Strategies to support E-safety:

- Pupils sign email appropriate usage policies.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Access in school to external personal email accounts will be blocked.
- Social email use can interfere with learning and may be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Pupils and staff emails monitored.

Website Monitoring and Safety

Our websites celebrate 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.

Social Networking

- The schools will block/filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM (Instant Messenger) and email addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas.
- Advice should be given regarding background detail in a photograph which could identify the student and his/her location e.g. house number, street name or school.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when a space has been set up without a password and others can see the comments.

Safeguarding Children Online

The school needs to help pupils to understand internet security through:

- Using safe online training websites.
- Encouraging them to report 'odd' events online.
- Discussing safety issues and modelling safe internet use.
- Reporting concerns immediately.
- Providing access to only appropriate web filtering and email monitoring systems.

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. The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioners Office, unless they are exempt. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them.

The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than necessary
- Processed in line with the individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

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.

Appropriate Usage Policies

All staff, parents, pupils and Governors have to read and sign a code of conduct when issued with their login.
All children in KS1 and KS2 sign an age specific E-Safety agreement.

Pupil's permission to use the Internet

Each child in Key Stage 1 and Key Stage 2 sign an age related E-Safety Agreement. Without this the child will be unable to use the internet within school.

Each year parents read and sign an internet code of conduct for their child.

- The school will maintain a current record of all staff and pupils who are not granted access to the school's electronic communications.
- All staff must read the e-safety policy before using any school ICT resource and sign appropriate use policy.
- At Reception and Key Stage 1, access to the internet will be by adult demonstration and occasionally directly supervised access to specific, approved online materials.
- Parents will be informed that pupils will be provided with supervised internet access.

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 the OCC filtering system management 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.

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.

Publication of the e-safety policy

- E-safety rules will be posted in key ICT areas.
- Pupils will be informed that network and internet use will be monitored.
- An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede internet access.
- All staff will be given the school e-safety policy and its application and importance explained.
- 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.

Parental Engagement

- Parents' attention will be drawn to the schools e-safety policy in newsletters and on the school website.
- E-safety resources linked on website for parents to access.
- Parents sign internet agreements and appropriate usage policies.
- 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 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.
- Parents are updated on contact information on a regular basis.