



POLICY DOCUMENT

Excellence Through Endeavour
"Let your Light Shine" – Matthew 5:16

ICT (Information and Communication Technology)
E-SAFETY POLICY

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.

Every Child Matters

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

1. Staying safe

Children need to be able to use the internet and school resources safely.

2. 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 supported to learn about making appropriate choices.

3. 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.

4. Making a positive contribution

Pupils need to be able to understand how to contribute to e-life in a safe environment.

5. 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 may 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 practice;
- 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 local authorities (LA) and national education authorities;
- Access to learning wherever and whenever convenient.

Accessing and evaluating information

We use a content filtering system provided by a Content Filter Provider (currently E2BN) to ensure inappropriate web material is not accessed through school resources. Access to sensitive sites, for example those that record the Holocaust, may be required for the duration of a specific educational activity by supervised pupils of appropriate age. The content filtering software can provide access to specific sites, which a teacher considers necessary for a particular purpose. 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.

- Virus protection will be updated regularly.
- Security strategies will be discussed with appropriate advisers.
- 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 e-mail.
- Files held on the school's network will be regularly checked.
- The ICT leader / Network Manager will review system capacity of the network regularly.

Principals of e-safety

- In school, as in industry, a member of staff who flouts security advice, 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 ensure 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 allegation of inappropriate behavior must be reported to the Designated Safeguarding Lead who will decide whether the incident requires further investigation as 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 all children can save their work in their own specific area of the system.

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 must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Any access by adults in school to external personal e-mail accounts must be carried out responsibly, ensuring accounts are closed immediately after use and screens are not left unsupervised.
- Social e-mail use can interfere with learning and may be restricted.
- E-mail 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.

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 and monitored by a nominated website manager.

Pupils' full names will not be used anywhere on the website in association with photographs.

Written permission from parents or carers will be obtained before images of pupils are electronically published.

Should any Teachers, Staff or Students find they have inadvertently accessed something that they should not of:

- Students need to make Teacher / Staff present at the time aware.
- Teacher / Staff need to make a note of URL / Web Address of Material accessed.
-
- ICT Co-Ordinator will then bring this to the attention of E2BN to be incorporated into the capture list.

Social Networking

- The school 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 e-mail 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 or 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 invite 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 setup without a password and others can see the comments.

Web Filtering

- The school will work with the Content Filter Provider to ensure that systems to protect pupils are regularly reviewed.
- If staff or pupils discover unsuitable sites, the web address must be reported to the ICT co-ordinator and in turn to the Content Filter Provider.
- The ICT co-ordinator / Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF (Internet Watch foundation) or CEOP (Child Exploitation and Online Protection Centre) (see appendix 1).
- The school's filtering strategy will be designed to suit the age and curriculum requirements of the pupils as advised by the Content Filter Provider.
- The ICT co-ordinator/ Network Manager will report any virus issues to the Content Filter Provider and/or RM (Research Machines) if necessary.

Video Conferencing

Video conferencing sessions at Sherington School are always led by a trained teacher. They ensure the session is planned and appropriate. Staff will consider safety aspects of the session.

The equipment must be secure and if necessary locked away when not in use.

- School video conferencing equipment should not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled.
- Video conferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- Establish dialogue with other conference participants before taking part in a video conference. If it is a non-school site, it is important to check that they are delivering material that is appropriate for your class.
- Teachers should report any issues to the ICT co-ordinator.

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 only to appropriate web filtering and email monitoring systems

Remote Learning Safety

The following should be considered when delivering virtual lessons, especially where webcams are involved:

- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred where possible.
- Lesson times should be kept to a reasonable length of time.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms provided and authorised by the school to communicate with pupils.

Practice considerations for staff members:

- Teachers and support staff should continue only to use school approved methods to communicate with pupils.
- Communications to take place during school hours.
- As per the ICT Acceptable Use Policy, staff should not use their private email addresses, WhatsApp groups or any other form of social media that is not directly regulated by the School to communicate with pupils.
- When communicating individually with pupils, staff should email via their school email address only and should copy in the Head Teacher.
- Staff should make the Head Teacher aware of when they will be using the school agreed platform (Teams for example).
- Staff members should avoid live 1:1 audio or video contact with individual pupils both to safeguard pupils and to safeguard themselves. If 1:1 contact cannot be avoided, permission to be gained from Head Teacher.
- Colleagues should use the school approved platform to upload pre-recorded video clips that they have made.

- In any recorded video, staff should ensure that no personal identifying information can be seen in the background. Dress should be appropriate, and the background should be appropriate and not contain any personal information.
- In all video footage recorded by teachers, people who are not connected to the school should not appear.

Practice considerations for live streaming of audio and visual content:

- Staff should only use school provided equipment for live-streaming sessions.
- At the start and throughout sessions, teachers should be clear about the expectations of student behaviour (e.g. a 'classroom standard' of behaviour is expected from all participants and they should usually mute their microphones unless they want to ask a question). Be clear that neither the recording by pupils nor the onward sharing of events is acceptable.
- Staff should make a note of the conference timing and who participated, including those that arrived/departed early or late.

Considerations for one to one lesson's:

- When using live video streaming facilities for one-to-one lessons, a responsible adult is always present to accompany the pupil for the lesson. The responsible adult must answer each call to show that they give their consent for the lesson to take place. They must then either remain in the room or nearby for the duration of the lesson, to ensure adequate supervision. No other children should be present, and teachers must end a lesson if there are other children visible.
- Teachers should only use school/organisation provided equipment for live-streaming sessions.
- Teachers should where possible record live sessions and store them in the agreed area (as detailed in school policy). The responsible adult and student should be made aware that this is happening.

Adoption of Prevent and Channel strategies

The school follows the guidance outlined in the Prevent and Channel Strategies. The Prevent strategy aims to stop people becoming terrorists or supporting terrorism. While it remains rare for children and young people to become involved in terrorist activity, young people from an early age can be exposed to terrorist & extremist influences or prejudiced views. As with other forms of safeguarding strategies, early intervention is always preferable. Schools, working with other local partners, families and communities, play a key role in ensuring young people and their communities are safe from the threat of terrorism.

Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Mobile phones will not be used during lessons or when supervising children unless cleared with the senior leadership team. Staff are expected to store their phones in their private belongings. If they are left in an area to which children have access they should be locked and not be accessible to the pupils. 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 these data can be very useful in improving services, data could be mishandled, stolen or misused. The General Data Protection Regulation (GDPR) 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 GDPR every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. The GDPR 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 GDPR sets standards (seven key principles), which must be satisfied when processing personal data (information that will identify a living individual). The GDPR also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them.

The GDPR sets out seven key principles which should lie at the heart of the school's approach to processing personal data:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Appropriate Usage Policies

All staff, parents, pupils and Governors have to read and signed an ICT code of conduct.

Pupils Permission to use the Internet

Parents will be distributed with the ICT Code of Conduct and asked to discuss and share with the child/ren. The signed copies will be returned to the office.

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff must read the e-safety policy before using any school ICT resource and sign an appropriate use policy
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

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 Content Filter Provider can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use annually to establish if the e-safety policy is adequate and that the implementation of the e-safety policy 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 member of the senior management team.
 - Informing parents or carers;
 - Removal of Internet or computer access for a period.

Publication of 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 and on the school e-Safety Policy will be provided as required.

Parental Engagement

- E-Safety resources are identified on the school website for parents to access through hyperlinks.
- Parents sign internet agreements and appropriate usage policies.
- 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.

Contacts

e-Safety Contacts and References

ChildLine <http://www.childline.org.uk/>

Child Exploitation & Online Protection Centre (CEOP) <http://www.ceop.gov.uk>

Internet Watch Foundation (IWF) <http://www.iwf.org.uk/>

Internet Safety Zone <http://www.internetsafetyzone.com/>

Childnet International <https://www.childnet.com/>

NSPCC <https://www.nspcc.org.uk/keeping-children-safe/online-safety/>

Think U Know website <http://www.thinkuknow.co.uk/>

Other links are available on the school website on the Online Safety for Parents page under the Parent menu. <https://www.shenington.oxon.sch.uk/online-safety-for-parents/>

This policy is in conjunction with the Parental Code of Conduct.