Orsett
Church of England
Primary School

E-SAFETY POLICY

Aims

⇒ To highlight the need to educate children, young people and their families about the benefits and risks of using new technologies such as mobile phones and Internet connected devices
⇒ To provide safeguards and rules to guide staff, pupils and visitors in their online experiences
⇒ The E-Safety Policy will operate in conjunction with others including policies for Behaviour, Anti-Bullying, Teaching and Learning, Safeguarding Children, Data Protection, Information Security, Acceptable Use and Use of Children's Images agreement

Effective Practice in E-Safety

E-Safety depends on effective practice in each of the following areas:

⇒ Education for responsible computer and mobile device use by staff and pupils
⇒ A comprehensive, agreed and implemented E-Safety Policy
⇒ Secure, filtered broadband from e2bn protex
⇒ A school network that complies with the National Education Network standards and specifications

E-Safety Audit

⇒ Orsett CE Primary School will undertake an annual E-Safety Audit to ensure effective practice is in place across the whole school. *(see Appendix 1)*

Writing and Reviewing the E-Safety Policy

⇒ The E-Safety Policy relates to other policies including those for Computing, bullying, child protection and data protection.
⇒ The school has an E-Safety Coordinator. This may be the Child Protection coordinator as the roles overlap. The role of E-Safety Coordinator is not a technical one.
⇒ Our E-Safety Policy has been written by the school, building on the Local Authority E-Safety Policy and government guidance.

TEACHING AND LEARNING

How does the Internet benefit education?

Benefits of using the Internet in education include:

⇒ Access to world-wide educational resources including museums and art galleries
⇒ Inclusion in government initiatives
⇒ Educational and cultural exchanges between pupils world-wide
⇒ Cultural, 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, professional associations and between colleagues
⇒ Improved access to technical support including remote management of networks and automatic system updates
⇒ Access to tools of direct communication, including video conferencing and email
⇒ Exchange of curriculum and administration data with Thurrock and DfE

How can Internet use enhance learning?

⇒ The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils
⇒ Pupils 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.
⇒ Access levels will be reviewed to reflect the curriculum requirements and age of pupils
⇒ Staff should guide pupils in on-line activities that will support the 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

How will pupils learn to evaluate Internet content?

⇒ If staff or pupils discover unsuitable sites the URL (address) and content must be reported to the Internet Service Provider via the Computing Subject Leader and the Child Protection Officer should be informed.
⇒ Pupils must follow the procedure for reporting unsuitable Internet content which is shared with all pupils by their class teacher
⇒ 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 and to respect copyright when using Internet material in their own work
⇒ The evaluation of on-line materials is a part of every subject

MANAGING INFORMATION SERVICES

How will our Computing system security be maintained?

⇒ The school Computing systems will be reviewed regularly with regard to security
⇒ Virus protection will be installed and updated regularly
⇒ Security strategies will be discussed with the Local Authority, particularly where a wide area network connection is being planned
⇒ Use of data storage facilities by pupils within school is checked by antivirus programs to protect against virus transfer
⇒ 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 scanned for virus and malware
⇒ The Computing Subject Leader/ Network Manager will ensure that the system has the capacity to take increased traffic caused by Internet use

How will e-mail be managed?

⇒ Each pupil has access to their own school-based server account, which is specific to their system login
⇒ Pupils must tell a teacher immediately if they receive offensive e-mail. The instance will be recorded by the System Administrator and appropriate sanctions applied
⇒ Pupils must not reveal personal details of themselves or those of others, or arrange to meet anyone in e-mail or other electronic communication, in line with E-Safety guidelines
⇒ Access in school to external pupil personal e-mail accounts is blocked
⇒ Excessive social e-mail use can interfere with learning and will be restricted
⇒ E-mails 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 messages is not permitted

How should Web site content be managed?

⇒ The point of contact on the Web site will be the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published
⇒ The Headteacher will take overall editorial responsibility and ensure content is accurate and appropriate on all pages directly related to the day-to-day workings of the school.
⇒ The Website should comply with the school's guidelines for publications
⇒ The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained

Can pupils' images or work be published?

⇒ Images which include pupils will be selected carefully and only those children whose written parental permission has been sought will be identifiable
⇒ Pupils' full names will not be used on the Website when associated with photographs, or in any way, which may be to the detriment of pupils.
⇒ Pupil photographs will immediately be removed from the school Website upon request from parents, or other appropriate request

How will social networking and personal publishing be managed?

⇒ The school will block 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 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. Pupils should be encouraged to invite known friends only and deny access to others
⇒ Pupils should be advised not to publish specific and detailed private thoughts
⇒ Teachers should be advised not to run social network spaces for pupil use on a personal basis
⇒ Newsgroups will not be made available unless an educational requirement for their use has been demonstrated.

How will filtering be managed?

⇒ The school will work in partnership with parents, Thurrock LA and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved
⇒ If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Computing Subject Leader and the child Protection Lead should be informed.
⇒ Senior staff 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 referred to the IWF or CEOP (please see references given later)
⇒ Filtering strategies will be selected by the school in discussion with the filtering provider where appropriate
⇒ Where possible, the filtering strategy will be selected to suit the age and curriculum requirements of pupils

How will videoconferencing be managed?

The equipment and network

⇒ If the school should decide to use videoconferencing the following will apply:
- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- All videoconferencing equipment in the classroom must be switched off when not in use
- External IP addresses should not be made available to other sites
- Videoconferencing contact information should not be put on the school Website
- School videoconferencing equipment should not be taken off school premises without permission.
- Use over the non-educational network cannot be monitored or controlled.

Users

⇒ Videoconferencing should be supervised appropriately for the pupils' age

⇒ Parental permission will be sought for children to take part in videoconferences

⇒ Only key administrators should be given access to the videoconferencing system, web or other remote control page

⇒ Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure

Content

⇒ When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference

⇒ Recorded material shall be stored securely

⇒ If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.

⇒ Videoconferencing 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 videoconference.

⇒ If it is a non school site it is important to check that they are delivering material that is appropriate for your class

How can emerging Internet uses be managed?

⇒ 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 formal school time. The sending of abusive or inappropriate text messages is forbidden.

⇒ The school should investigate wireless, infra-red and Bluetooth communication technologies and decide a Policy on phone use in school.

⇒ The sending of abusive or inappropriate text messages is forbidden. To ensure this students may not use the school network to send text messages nor may they use instant messaging.

How should personal data be protected?

⇒ Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Orsett
Church of England
Primary School

POLICY DECISIONS

How will Internet access be authorised?

⇒ All staff and pupils will initially be granted Internet access
⇒ Parents/carers will be informed that pupils will be provided with supervised Internet access
⇒ Parents / carers will sign a consent form giving their permission for their child to use the Internet in school *(Acceptable Use Policy – pupils)*
⇒ Pupils will sign an E-Safety agreement form indicating they are aware of the rules of conduct when using the Internet and other Computing resources *Acceptable Use Policy – pupils)*
⇒ The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
⇒ Pupils will not be allowed to use computers with Internet unless they are directly supervised by a member of staff
⇒ Guidelines relating to Internet safety are visible from all machines with Internet access, throughout the school

How will the risks be assessed?

⇒ In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and linked 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 Thurrock Borough Council can accept liability for the material accessed, or any consequences resulting from Internet use.
⇒ 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
⇒ The Headteacher will ensure that the E-Safety Policy is implemented and compliance with the Policy monitored

How will E-Safety complaints be handled?

⇒ Responsibility for handling incidents will be delegated by the named safeguarding member of staff
⇒ Any complaint about staff misuse must be referred to the Headteacher
⇒ Pupils and parents will be informed of the complaints procedure
⇒ Parents and pupils will need to work in partnership with staff to resolve issues
⇒ There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies
⇒ Sanctions available include:
    - interview/counselling by senior member of staff/class teacher/teaching assistants;
    - informing parents or carers;
    - removal of Internet or computer access for a period, which could prevent access to school work held on the system.

How is the Internet used across the community?

⇒ The school will liaise with local organisations to establish a common approach to E-Safety
⇒ The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice

Orsett
Church of England
Primary School

COMMUNICATIONS

How will the Policy be introduced to pupils?

⇒ Rules for Internet access will be posted on or near all computer systems with Internet access
⇒ An E-Safety training programme will be introduced to raise the awareness and importance of safe and responsible Internet use both at school and home
⇒ Internet safety guidelines will be prominently linked from the home page of the school's intranet and Internet sites
⇒ Pupils will be informed that Internet use will be monitored
⇒ Instruction in responsible and safe use should precede Internet access

How will the Policy be discussed with staff?

⇒ 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
⇒ The monitoring of Internet use is a sensitive matter. Staff should only operate monitoring procedures on instruction from the Senior Leadership Team
⇒ Staff training in safe and responsible Internet use, and on the school E-Safety Policy will be provided as required

How will parents' support be enlisted?

⇒ Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school prospectus and on the school website
⇒ Internet issues will be handled sensitively to inform parents without undue alarm
⇒ A partnership approach with parents will be encouraged. This will include leaflet distributions, demonstrations, practical sessions and suggestions for safe Internet use at home
⇒ Interested parents will be referred to relevant organisations on request

Other documents

See also:

- Teaching and Learning Policy
- Behaviour Policy
- Anti-bullying Policy
- Safeguarding Children Policy
- Data Protection Act 1998
- Use of children's images agreement
- Acceptable Use Policy
- Computing policy

Ratified by Governors: June 2016

Review Date: June 2018

Orsett
Church of England
Primary School

Appendix 1

E-SAFETY AUDIT

This audit should be completed by the member of the Senior Leadership Team (SLT) responsible for the E-Safety Policy. Staff who could contribute to the audit include the Designated Person for Child Protection, Data Protection Officer, Data Security Officer, SENCO, E-Safety Coordinator, ICT Subject Leader and Headteacher.

Has the school an E-Safety Policy that complies with Thurrock guidance?	**Yes**
Date of latest update *(Annually)*	***March 2016***
The school E-Safety Policy was agreed by governors on	***June 2016***
The Policy is available for staff	***Staff Handbook***
The Policy is available for parents/carers	***On wesite***
Member of the Senior Leadership Team responsible for E-Safety	**Computing SL**
Member of the Governing Body responsible for E-Safety	**Chair of F&P**
Designated Person for Child Protection	**Headteacher**
Data Protection Officer	**Headteacher**
E-Safety Coordinator	**Headteacher**
Has E-Safety training been provided for all staff?	**Yes-2015**
Has E-Safety guidance been provided for all pupils?	**Yes-2015**
Are E-Safety guidance materials available for parents?	**Yes**
Is there a clear procedure for a response to an incident of concern?	**Yes**
Have E-Safety materials from CEOP and Becta been considered?	**Yes**
Do all staff sign an Acceptable Use Policy on appointment?	**Yes**
Have all pupils signed an E-Safety agreement form?	**Yes**
Have all parents/carers signed an E-Safety home/school agreement form?	**Yes**
Are E-Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	**Yes**
Has an ICT security audit been initiated by SLT?	**Yes**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Yes**
Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements (e.g. LGfL)?	**Yes**
Has filtering on Internet-based devices been appropriately applied?	**Yes**