Forest Academy

&

Elveden Church of England Primary Academy

E-Safety Policy

Date Completed: March 2015

Completed by: R King

Review Date: March 2016

1. Who will write and review the policy?

The school's ICT and PSHE leaders will work in collaboration with the Senior Leadership team in order to ensure this policy meets the ever-changing issues relating to the Internet and its safe use. Our e-safety Policy has been written by the school, building on government guidance. The policy has been agreed by the leadership team and approved by the Governing Body. It will be reviewed regularly. Changes will be made immediately if technological or other developments so require.

2. What is e-Safety?

- E-Safety encompasses Internet technologies and electronic communications such as mobile phones. This policy highlights the need to educate pupils about the benefits and risks of using technology, enabling users to control their online experiences.
- The previous policy; 'Internet and email Policy', has been revised and renamed as the school's e-safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.
- This policy will operate in conjunction with other school policies including those for ICT, behaviour, bullying, PSHE and child protection.
- This policy has been developed following guidance issued by the Children, Families and Education Directorate.

TEACHING & LEARNING

3. Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is a part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

4. 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 such as the National Grid for Learning (NGfL) and the Virtual Teacher Centre (VTC) and ICT Mark (Becta);
- 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.

5. 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.

6. What should the e-safety curriculum for pupils include?
- The schools planned e-safety curriculum should be taught, revisited and referred to through linked ICT and PSHE lessons.
- Key messages about e-safety are taught and revisited through whole school or key stage assemblies. The school also takes part in the annual SID.
- Where internet use is planned, school staff should ensure that children are reminded of class/ key stage internet use rules.

7. 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 ICT Subject Leader. Pupils must follow the procedure for reporting unsuitable Internet content (Appendix I) 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

7 How will our ICT system security be maintained?
- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Use of data storage facilities by pupils within school is prohibited 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 checked by the Network manager and ICT leaders?
- The ICT Subject Leader/ Network Manager will ensure that the system has the capacity to take increased traffic caused by Internet use.
- Documents containing 2 or more pieces of personal information must be password protected.

8 How will e-mail be managed?
- Each pupil has access to their own school-based email account, which is specific to their system login through our DBPrimary VLE. Children are able to send emails internally (for external email addresses see below). These emails can be monitored by class teachers and System Administrators.
- 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 their personal details 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 personal e-mail accounts is blocked.
- Excessive social e-mail use can interfere with learning and may 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.

9 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.

10 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.

11 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. Students 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.

12 How will filtering be managed?
- The school will work in partnership with parents, Becta 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 ICT Subject Leader.
- 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 CEOP, linked from the website.
- 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.

13 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 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.

14 How should personal data be protected?
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

POLICY DECISIONS

16 How will Internet access be authorised?
- All staff and pupils will initially be granted Internet access.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form.
- 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.

17 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. The school cannot 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.
- All staff will need to sign the Acceptable use policy, showing that they understand the risks and need for safer internet use in line with professional standards.

- Parents and pupils will also be sent an acceptable use policy showing key ways in which they can reduce the risks of misusing the internet.

18 Responding to incidents of misuse or e-safety complaints.
- Responsibility for handling incidents will be delegated to a senior member of staff or the e-safety leader.
- 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.
- When responding to an incident reported by a pupil, member of the staff, or parent relating to a child in the school, the reporting of e-safety incident forms should be used and referred to the SDP/ ADP or e-safety leader. (See attached flow chart for additional guidance - appendix 1)
- For incidents that take place outside of school, a link to the suggested CEOP site 'report abuse' page is available from the links section of the school website..

Sanctions available include:
- Investigate all incidents.
- Interview/counselling by senior member of staff/class teacher/teaching assistants;
- Informing parents or carers through letters home and meetings;
- Record all incidents or bullying and monitor.
- Listen and support all concerned.
- Removal of Internet or computer access for a period, which could prevent access to school work held on the system.
- Suggest strategies and ways forward.
- Review the situation and check for progress.
- For incidents where an illegal action has occurred CEOP forms will be filled in and an incident report form will be completed in line with the Suffolk E-Safety flow chart.

19 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.

COMMUNICATIONS POLICY

20 How will the policy be introduced to pupils?
- Rules for Internet access will be posted on or near all computer systems with Internet access, these will be written by individual classes and also displayed inside the classroom.
- E-safety education is embedded throughout the new ICT curriculum 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 websites
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- A child friendly version of the school's safeguarding policy has been written and shared with children – this includes specific reference to safe use of technologies and the internet.

21 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 Leadership Team.
- Staff training in safe and responsible Internet use, and on the school e-Safety Policy, will be provided as required.

22 How will parents' support be enlisted?
- Parents' attention will be drawn to the School e-Safety Policy in newsletters 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 organisations listed in Appendix II.