Stoke Row CE School

E-Safety Policy

Document Approval Record

Committee	Teaching and Learning
Chair of Committee	Ryan Bradley
Approval Date	April 2018
Review Date	April 2021
	Annual? ¥ / N

FGB Approval:

Headteacher	Charlotte Harris
Chair of Governors	David Lowe
Approval Date	26th April 2018

These policies are all created in line with the Christian foundation of this school which is expressed through our five core values and our view that every child is unique and valued.

Contents

1 Introduction

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and games consoles, as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Stoke Row has created this e-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole. Pupils need to learn safety rules in a way that does not frighten them and which gives them confidence to know what to do in certain situations. Pupils need to understand that certain rules will change and develop as they get older.

The school's e-safety policy will operate in conjunction with other policies including those for Pupil Discipline, Home-School Agreement, Curriculum and Data Protection Policy, Data Retention Policy and Data Breach Policy.. Staff should also be aware of Oxfordshire County Council's Acceptable Use policy.

1.1 Why Internet use is important

- 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 need to learn how to evaluate Internet information and to take care of their own safety and security.
- 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 staff and pupils.

1.2 How Internet use can benefit education

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils worldwide;
- 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 networks of schools, 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 with OCC and DfE;
- access to learning wherever and whenever convenient.

1.3 Internet use will enhance learning

- The school's Internet access will be designed to enhance and extend education
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Staff will guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

1.4 Pupils will be taught how to evaluate Internet content

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

2 Managing Internet Access

2.1 Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Pupils may only download files approved by a teacher.
- All downloaded files must be virus checked before use.

2.2 E-mail

- Pupils do not have a school e-mail account
- Any e-mail sent to an external organisation should be written carefully in the same way as a letter written on school headed paper.
- An e-mail disclaimer with the wording, '*This e-mail and any attachments are intended only for the recipients listed. If it has come to you in error please delete it and let us know. This message and its attachments have been scanned for viruses but we cannot guarantee them to be virus free'* will be included at the bottom of all school e-mail accounts.

2.3 Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

2.4 Publishing pupil's images and work

- Images or videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- 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 photographs of pupils are published on the school website (see Stoke Row's Home-School Agreement and GDPR signed agreement).
- A pupil's work can only be published with the permission of the pupil or parents (see Stoke Row's Home-School Agreement).

2.5 Social networking and personal publishing

- Pupils will be advised never to give out personal details (their own or another person's) of any kind which may identify them or their location.
- Pupils will be advised not to upload photographs or videos of themselves or other pupils.
- Pupils will be advised to use an anonymous "cyber-name" when on the internet. Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords (see Appendix B), deny access to unknown individuals and to block unwanted communications. All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

2.6 Managing filtering

- The school will access the Internet by means of our ISP Turn IT On, which provides an appropriately filtered service. If staff or pupils discover an unsuitable site, it must be reported to the Headteacher who will speak to our ICT support systems to ensure this it is no longer viewable.

2.7 Managing emerging technologies

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

2.8 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR 25th May 2018.

3 Policy Decisions

3.1 Authorising Internet access

- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- Parents will be asked to sign and return a consent form (see Stoke Row's Home-School Agreement).
- At Foundation Stage and Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.
- A tool is available on all computers for pupils to immediately press if they see something they don't like online and it will blur the screen until the teacher is able to come over and assist.

3.2 Assessing risks

- 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 unsuitable material will never appear on a school computer. Neither the school nor OCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Oxfordshire Police.
- All members of staff will be required to read and sign the Acceptable Users Policy as part of their induction process.
- Methods to identify, assess and minimise risks will be reviewed regularly.

3.3 Responding to any incidents of concern

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content, etc.).
- The Headteacher will record all reported incidents and actions taken in the school behaviour log and report it to our ICT support service, 'Turn IT On'. The designated safeguarding lead will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school's behaviour and anti-bullying policies where appropriate.

- The school will inform parents/carers of any incidents or concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the OCC School's Safeguarding Team and escalate the concern to the Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the OCC School's Safeguarding Team.

3.4 Handling e-safety complaints

- Complaints about Internet misuse will be dealt with under the school's complaints procedure.
- Any complaint about staff misuse must be referred to the Headteacher.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

3.5 Managing Cyberbullying

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policies on anti-bullying and behaviour.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate.
- The school will intervene with any incidents of online bullying even when this has occurred outside of school hours.

3.6 Managing the mobile phones and personal devices

- Staff mobile phones and personal devices will not be used during lessons or formal school time.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Pupils are not allowed any personal mobile devices in school.

3.7 Introducing the e-Safety policy to pupils

- Pupil instruction regarding responsible and safe use will precede Internet access.
- e-Safety rules (see Appendix 1) will be posted in all classrooms and discussed with the pupils at the start of each year.

- Pupils will be informed that network and Internet use will be monitored.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- All children will take part in Internet Safety Day annually as this is part of our curriculum cycle. Each year observes a different theme which we will follow.

3.8 Staff and the e-Safety policy

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

3.9 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting e–Safety at other attended events. Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.

3.10 e-Safety Resources

- The following websites are useful in supporting learning about e-safety:
- Child Exploitation and Online Protection (CEOP) Centre
  www.ceop.police.uk
- UK Council for Child Internet Safety (UKCCIS)
  http://www.education.gov.uk/ukccis
- Think U Know
  www.thinkuknow.co.uk

APPENDIX A: Passwords

A.1 How to choose a good password

The following guidelines may be used to aid the selection of a good password:-

- Use at least 8 characters.
- The more characters, the better (as long as you can remember them).
- It should contain characters from at least three of the following groups :-
    - Upper case letters
    - Lower case letters
    - Numbers
    - Special characters - !@#£$%^&*(),./?;[=] etcetera (except where the application or operating system limits the characters which may be used)
- Make your password easy for you to remember but hard for someone else to guess.

Picking letters from a phrase that's meaningful to you may be the source for a good password. In this way, your password is really a "pass phrase." ("Do you know the way to San Jose?" could be D!Y!KtwTSJ?). The following strategies may be useful when creating a strong password:-

- Use lines from a childhood verse.
  Verse Line: Yankee Doodle went to town
  Password: YDwto#town
- Expressions inspired by the name of a city.
  City Expression: I love Paris in the springtime
  Password: ILp!nST
  City Expression: Chicago is my kind of town
  Password: CimYK0t
- Foods disliked during childhood.
  Food: rice and raisin pudding
  Password: ric+raiPudng
  Food: boiled broccoli
  Password: boi%Brocc
- Transformation techniques.
    - Technique: Transliteration
      Illustrative Expression: photographic
      Password: foT()grafik
    - Technique: Interweaving of characters in successive words.
      Illustrative Expression: iron horse
      Password: ihrOrnSe#
      Illustrative Expression: file drawer
      Password: Fd1rLawer
    - Technique: Substitution of synonyms.
      Illustrative Expression: coffee break
      Password: jaVa^rest
    - Technique: Substitution of antonyms.
      Illustrative Expression: stoplight
      Password: star*Tdark
    - Technique: Sequence of unrelated words,
      Illustrative Expression: crock irk resin
      Password: cr#ckIRKre$In

Note: Obviously, you shouldn't use any of the passwords used as examples in this document. Treat these examples as guidelines only.