Stoke Row CE School

E-Safety Policy

Document Approval Record

Committee	Teaching and Learning
Chair of Committee	Ryan Bradley
Approval Date	June 2015
Review Date	April 2018
	Annual? ¥ / N

FGB Approval:

Headteacher	Charlotte Harris
Chair of Governors	David Lowe
Approval Date	June 2015

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 at low cost. 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. This policy document has been created from a model policy, the original of which can be found on the Kent Trust Web under 0-24 Learning and Curriculum – ICT Strategy – E-safety

There is an underlying assumption that children have both understanding and application of "safety". Pupils need to understand that rules given to them must be followed. 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. Staff should also be aware of Oxfordshire County Council's Acceptable Use Policy (which may be found on Insite under:
About us – Governance – Corporate governance library – Use of ICT).

2 Teaching and Learning

2.1 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.

2.2 How Internet use can benefit education

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- 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.

2.3 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.

2.4 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.

3 Managing Internet Access

3.1 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.
  (Note: this includes files loaded from external media, e.g. CD, Memory Stick, etc., as well as from the Internet.)
- All downloaded files must be virus checked before use.

3.2 E-mail

- Pupils may only use approved e-mail accounts on the school system.
- 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.
- E-mail sent to an external organisation 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.

3.3 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.

3.4 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 Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site (see Stoke Row's Home-School Agreement).
- Pupil's work can only be published with the permission of the pupil or parents (see Stoke Row's Home-School Agreement).

3.5 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 logging onto sites external to the OCN.
- 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. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- 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.

3.6 Managing filtering

- The school will accesses the Internet by means of the Oxfordshire Community Network (OCN), which provides an appropriately filtered service.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator.

3.7 Managing videoconferencing

- Videoconferencing is not used at Stoke Row School.

3.8 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.

3.9 Protecting personal data

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

4 Policy Decisions

4.1 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 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.

4.2 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.
- Methods to identify, assess and minimise risks will be reviewed regularly

4.3 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 e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The designated Child Protection Coordinator 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 of 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 Safeguard 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 Safeguard Team.

4.4 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.

4.5 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.

4.6 Managing the Learning Platform

- SLT and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, parent/carers, staff and governor community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, pupils etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

4.7 Managing the mobile phones and personal devices

- Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times.
- 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. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

5 Communications Policy

5.1 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.

5.2 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.

5.3 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- 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 e.g. parent evenings and sports days.

- Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement

5.4 e-Safety Resources

- The following three Becta e-safety publications are available on the Oxfordshire Learning Platform (in the document library of the Stoke Row Staff Room interest space) and online:
    - Signposts to safety: Teaching e-safety at Key Stages 1 and 2 https://www.education.gov.uk/publications/standard/publicationDetail/Page1/BEC1-15488
    - Next Generation Learning – Safeguarding learners http://teachfind.com/becta/about-becta-publications-safeguard-learners-online-how-are-you-safeguarding-next-generation-le?current_search=becta%20safeguarding
    - Safeguarding children online - Are you managing online risks well? http://webarchive.nationalarchives.gov.uk/20101102103654/publications.becta.org.uk//display.cfm?resID=42194
- Child Exploitation and Online Protection (CEOP) Centre www.ceop.police.uk
- UK Council for Child Internet Safety (UKCCIS) http://www.education.gov.uk/ukccis
- Get Safe Online http://www.getsafeonline.org/nqcontent.cfm?a_name=beginners_1
- Think U Know www.thinkuknow.co.uk
- Know IT All for Primary Schools http://childnet-int.org/kia/primary/

APPENDIX A: e-Safety Rules

Stoke Row CE Primary School e-Safety Rules

You are responsible for good behaviour on the Internet just as you are in all other aspects of life at school. Communications via the Internet, e.g. email, should not be thought of as private. The e-Safety Rules apply at all times, in and out of school hours, whilst using school equipment.

The use of information and communication technologies (ICT), including the Internet, is provided for you to get information and to communicate with others if you agree to act in a considerate and responsible manner. This use is a privilege and not a right and you need to be responsible. It is expected that you will comply with these codes.

During lessons teachers will guide you. Outside lesson time you must only access sites that are appropriate for school and when there is a school adult in the room.

e-Safety Rules for Key Stage 1

- We only use the internet when an adult is with us.
- We can click on the buttons or links when we know what they do.
- We can search the Internet with an adult.
- We always ask if we get lost on the Internet.
- We can send and open emails together.
- We can write polite and friendly emails to people that we know.

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we are not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We only download files an adult has approved.
- We do not use Internet chat rooms.

APPENDIX B: Passwords

B.1 Why use passwords?

Passwords are often the first (and possibly only) defence against intrusion. They protect personal information – information we don't want anyone and everyone to know. In our personal lives, this means financial information, health data, and private documents. In a professional context, this may encompass anything considered crucial to the success of the organization: pupil details, financial data, etc.

Passwords are simpler and cheaper than other, more secure forms of authentication like special key cards, fingerprint ID machines, and retinal scanners. They provide a simple, direct means of protecting a system or account. Passwords are generally used in combination with some form of identification, such as a username, account number, or e-mail address. While a username establishes the identity of the user for the computer or system, the password, which is known only to the authorized user, authenticates that the user is who he or she claims to be. This means that their function is to "prove to the system that you are who you say you are".

B.2 Password Cracking

While passwords are a vital component of system security, they can be cracked or broken relatively easily. Password cracking is the process of figuring out or breaking passwords in order to gain unauthorized entrance to a system or account. Passwords can be cracked in a variety of different ways. The simplest is the use of a word list or dictionary program to break the password by brute force. These programs compare lists of words or character combinations against a password until they find a match.

Another easy way for potential intruders to obtain passwords is through social engineering: watching a password being typed, physically reading the password off a Post-It from under someone's keyboard or through imitating an IT engineer and asking over the phone (phishing). Many users create passwords that can be guessed, simply by learning a minimal amount of information about the person whose password is being sought. A more technical way of learning passwords is through sniffers, which look at the raw data transmitted across the net and decipher its contents. A sniffer can read every keystroke sent out from your machine, including passwords.

B.3 What makes a good password?

A weak password is any password that can easily be guessed or cracked. A strong password is difficult to crack or guess. A bad password is one that is too weak for the resources it is supposed to defend or that is too difficult for users to use and remember. A good password is a strong password that's reasonably easy to remember.

So a password needs to be :-

- Strong
  (computationally difficult - to avoid brute force attack)
- Hard to guess
  (obscurity is an asset - avoid the obvious)
- Easily remembered
  (so there is no need to write it down)
- Changed periodically
  (to limit time at risk)

- Unique
  (not reused on several accounts)
- Kept secret

B.4 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 springtim
  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.

B.5 How to avoid a bad password

To avoid a weak password that would be easy to crack, do not use :-

- Dictionary words.
  (mackerel, dandelion, millionaire)
- Foreign words.
  (octobre, gesundheit, sayonara)
- Simple transformations of words.
  (tiny8, 7eleven, dude!)
- Names (things or people, real or fantasy), doubled names, initials, first name and last initial, initials and last name.
  (mabell, kittykitty, rcog, marissab, hgwells)
- Uppercase or lowercase words.
  (MAGAZINE, liquorice)
- An alphabet sequence, (lmnop)
  a numeric sequence, (1111122222, 0987654)
  or a keyboard sequence. (ghjkl;)
- Very short words or just one character.
  (dog, *, hi!, me, love)
- Words that have the vowels removed.
  (sbtrctn, cntrl, ntllgnc)
- Phone numbers, PIN numbers, car licence plates, etc.
- A network login ID in any form.
  (e.g. all lower case, all upper case, reversed order, etc.)
- Passwords that are easily guessed by people that know you.
  (e.g. middle names, street addresses, phone numbers, children's ages or names, pets' names, and so on)

B.6 Password Management

Having followed the guidelines in this document to create a strong password you should endeavour to keep it secret :-

- If you write your password down, be VERY careful where it's stored.
  Avoid the "mousepad safe".
- Never e-mail your password to anyone.
  Beware the "phisher".
  E-mail is not secure.
- Don't tell anyone else your password.
- Don't enable the "password save" option on software.
- Don't reuse the same two or three passwords in rotation.
- If you think your password is compromised, contact your system administrator immediately.

You should change your password if :-

- You have had the same password for more than 6 months.
- You have told your password to anyone else.

- You have visited another school or location and logged on to a system there.
- You are officially notified that your password does not meet current standards.

When creating or changing a password it is a good idea to spend some time practicing it, to help commit it to memory. You could try :-

- Repeatedly logging in and out of the system.
- Writing the password down several times, and then shredding the paper.
- Repeatedly typing the password into a new Word document, and then discarding (not saving) the document.

Under normal circumstances, ordinary user passwords should never be written down (or shared) because an administrator can always give the user a new password (which the user may or may not have to change) whenever a password is forgotten. However, it is recommended that administrator passwords (with their associated account names) are written down, placed in a sealed envelope and kept in secure, non-personal, storage facilities, because it is not possible to reset an administrator's password in the same way as a user's password. The document must be updated as existing passwords are changed and new ones are created because its main use will be as a backup for forgotten passwords.