This policy has been written in working with children, staff and parents of St. Matthew's Primary School. It is an adaptation and personalisation of a model policy drafted by the Kent County Council e-Safety Policy and government guidance. It has been agreed by the Senior Leadership Team and approved by governors.

Contents

Section 1 - Teaching and learning

a) Why is Internet use important?

Internet use is part of the statutory curriculum and an important tool for learning.

The Internet is a part of everyday 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 access is an entitlement for students who show a responsible and mature approach to its use.
- All year groups are taught units that focus specifically on e-Safety, including our digital footprint and cyber bullying.

b) How does Internet use benefit education?

The 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
- access to learning wherever and whenever convenient.

c) How can Internet use 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 copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

- Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity.
- As part of units on Computer Science and Digital Literacy, 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.

d) How will pupils learn how to evaluate Internet content?

Pupils at KS2 should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The evaluation of online materials is a part of teaching/learning across the curriculum.

Section 2 - Managing Information Systems

a) How will information systems security be maintained?

The security of the school information systems and users will be reviewed regularly.

Virus protection will be updated regularly.

Staff Passwords will be "strong" (Appendix G – Creating Strong Passwords)

b) How will email be managed?

Children can only communicate with other children in their class, plus staff associated with their class, through eschools. These communications can be monitored to make sure that they are appropriate.

Pupils must immediately tell a teacher if they receive offensive email. Children can do this by pressing the "Report This" button on every message they receive.

Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

- Staff should only use eschools email accounts to communicate with pupils.
- Staff should not use personal email accounts during school hours (excluding non directed / lunchtime / after school) or for professional purposes.
- All school related email communications by staff and governors should be conducted through their "@stmatthews.cambs.sch.uk" email accounts
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

c) How will published content be managed?

The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.

- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

d) Can pupil's images or work be published?

Images that include pupils will be selected carefully.

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

Permission is sought from parents or carers via the school admission form before images of pupils are electronically published.

e) How will social networking, social media and personal publishing be managed?

Children will not be allowed to use any social networking sites, other than eschools. Eschools provides one of the safest platforms available for children to learn about communicating safely online. Eschools is a "closed" system, meaning that children can only communicate with other children in their class, plus staff associated with their class, through eschools. These communications can be monitored to make sure that they are appropriate.

Pupils will be taught 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 email addresses, full names of friends/family, specific interests and clubs etc.

- As part of the e-Safety curriculum, pupils will be taught about the issues when using social networking sites. Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and be taught about privacy settings. Advice should be given regarding background detail in a photograph which could identify the student or his/her location. Pupils will also be taught that they should only communicate online with people that they already know.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team.
- Staff will not discuss pupils, staff or the school on social networking sites.
- If personal publishing is to be used with pupils then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site should be moderated by school staff.
- Pupils should be taught how to set passwords and the principles of staying safe online.
- Pupils are taught not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

f) How will filtering be managed?

St Matthews uses the county provided filtering service, which ensures that systems to protect pupils are reviewed and improved.

If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Coordinator and ictsupport@stmatthews.cambs.sch.uk (Appendix E – e-Safety incident reporting form)

The school's broadband access will include filtering appropriate to the age and maturity of pupils. This service is provided by Cambridgeshire County Council.

- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network manager.

g) How will videoconferencing be managed?

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

Video conferencing will only be used in a group situation under the control of a member of staff. Only providers approved by CCC will be used by staff. CCC approved provider is the regional broadband consortium E2BN. Details of the service can be found here
http://www.e2bn.org/services/25/video-conferencing.html

Staff will be issued with a school phone where contact with pupils is required.

- Mobile phones will not be used during lessons or formal school time, except where use of a mobile phone is necessary, such as on an educational visit, or in the event of an emergency. The sending of abusive or inappropriate text, picture or video messages is forbidden.
- Staff will not use mobile phones to take photographs of children.

h) *How should personal data be protected?*

- Personal data will be recorded, processed, transferred and made available according to the school's Data Protection Policy.
- All school laptops will be encrypted to protect any personal data held on the laptop.
- Flashdrives will generally not be used for storing personal data and, in exceptional circumstances where this is necessary, the flashdrive will be encrypted.

Policy Decisions

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 and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource. (Appendix A – Staff Code of Conduct)

a) How will risks be assessed?

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. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.

The school will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate. This will be done in response to any significant changes in legislation, technology or in response to incidents in school or nationally. It will also be done in accordance with the review schedule for the e-Safety policy.

- 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.

b) How will e–Safety complaints be handled?

Complaints of 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.

- The School's Complains Procedure is accessible via the school's website.
- Parents and pupils will work in partnership with staff to resolve issues.
- Discussions will be held in the first instance with Local Authority Senior Education Officers to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's behaviour managements and safeguarding procedures.

c) How will Cyberbullying be managed?

Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set

out in the school's policy on anti-bullying.

There will be clear procedures in place to support anyone affected by Cyberbullying.

- All incidents of cyberbullying reported to the school will be recorded.
- Incidents or allegations of Cyberbullying will be responded to in accordance with the anti-bullying policy
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in Cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content.
    - Internet access may be suspended at school for the user for a period of time.
    - Parent/carers will be informed.
    - The Police will be contacted if a criminal offence is suspected.

e) How will Learning Platforms and learning environments be managed?

SLT and staff will monitor the usage of eschools by pupils and staff regularly in all areas, in particular message and communication tools and publishing facilities.

Pupils/staff will be advised on acceptable conduct and use when using eschools. Pupils will sign to accept the rules of use.

Only members of the current pupil, parent/carers and staff community will have access to eschools.

All users will be mindful of copyright issues and will only upload appropriate content onto eschools.

When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

- Any concerns with content may be recorded and dealt with in the following ways:

    a) The user will be asked to remove any material deemed to be inappropriate or offensive.

    b) The material will be removed by the site administrator if the user does not comply.

    c) Access to eschools for the user may be suspended.

    d) The user will need to discuss the issues with a member of SLT before reinstatement.

    e) A pupil's parent/carer may be informed.

- A visitor may be invited onto the eschools by a member of the SLT. In this instance there may be an agreed focus or a limited time slot. Access will only be provided to the relevant sections and personal data will be protected.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

Section 4 - Communication Policy

a) How will the policy be introduced to pupils?

All users 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.

- Pupil instruction in responsible and safe use should precede Internet access. (Appendix B and C – Key Stage 1 & 2 Rules, Appendix C – Child Contract, Appendix F – Suggested Websites for e-Safety Training)
- An e-Safety module will be included in Computing Curriculum.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.

b) How will the policy be discussed with staff?

The e-Safety Policy will be formally provided to and discussed with all members of staff. This forms part of the staff induction process.

To protect all staff and pupils, the school will implement acceptable use frameworks.

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 the Senior Leadership Team and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use both professionally and personally will be provided.

c) How will parents' support be enlisted?

Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school website.

- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use or highlighting e-Safety at other attended events e.g. parent evenings, sports days.
- Acceptable use and e-Safety forms part of the home school agreement.
- Information and guidance for parents on e-Safety will be made available to parents on the school website.

Section 4 - e-Safety Contacts and References

Cambridge ICT Service - http://www.theictservice.org.uk/

Cambridge e-Safety service - http://www.ccc-e-Safety.org.uk/site

Becta: *www.becta.org.uk/safeguarding*

CEOP (Child Exploitation and Online Protection Centre)*: www.ceop.police.uk*

Childline: *www.childline.org.uk*

Childnet: *www.childnet.com*

Click Clever Click Safe Campaign: *http://clickcleverclicksafe.direct.gov.uk*

Cybermentors: *www.cybermentors.org.uk*

Digizen: *www.digizen.org.uk*

EIS - ICT Support for Schools and ICT Security Advice: *www.eiskent.co.uk?ictsecurity*

Internet Watch Foundation: *www.iwf.org.uk*

http://ccc-e-Safety.org.uk/website/getting_a_clear_picture_/50616

Kidsmart: *www.kidsmart.org.uk*

Teach Today: *http://en.teachtoday.eu*

Think U Know website: *www.thinkuknow.co.uk*

Virtual Global Taskforce — Report Abuse: *www.virtualglobaltaskforce.com*

Appendix A - Staff Code Of Conduct

Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-Safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the e-Safety Coordinator, the Designated Child Protection Coordinator or Headteacher.
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-Safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

All staff sign a safeguarding declaration form when joining St Matthew's. In signing this form staff confirm that they have read this safety policy, have read this Code of Conduct and agree to abide by it.

Appendix B - Reception and Key Stage 1 Rules

Think then Click

These rules help us to stay safe on the Internet

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.

B. Stoneham & J. Barrett

Using eSchools

1. I promise to keep my password secret.
2. I know everything I do can be seen by my teacher.
3. We always follow the five golden rules of the school on the internet - "no swearing, teasing or name-calling"
4. We don't waste time with silly messages, blogs or chats.
5. We tell our teacher or parent if we think someone is breaking the rules.
6. We click "report this" if we get a message that breaks the rules.

Remember – You can be taken off eSchools if you break the rules.

Appendix C - Key Stage 2 Rules

Think then Click

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 tell an adult about 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, or talk to anyone, we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

Using eSchools

1. I promise to keep my password secret.
2. I know everything I do can be seen by my teacher.
3. We always follow the five golden rules of the school on the internet - "no swearing, teasing or name-calling"
4. We don't waste time with silly messages, blogs or chats.
5. We tell our teacher or parent if we think someone is breaking the rules.
6. We click "report this" if we get a message that breaks the rules.

Remember – You can be taken off eSchools if you break the rules.

Appendix D - Child contract / Parental Consent - The following text is part of our Home/School Agreement

St Matthew's Primary School
e-Safety Agreement

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil: **Class:**

Pupil's Agreement

- I have read and I understand the school e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed: **Date:**

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the school e-Safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: **Date:**

Please print name:

Please complete, sign and return to the school office.

Appendix E – e-Safety Incident Reporting Form

Date of incident:	
Member of staff reporting incident:	
Url, (web address) of incident:	
Copy of screens/evidence saved to:	
Location of incident (room):	
Computer number if known:	
Details:	
Passed to:	
Action taken:	

Appendix F - Suggested websites for e-Safety teaching

- Think U Know: ***www.thinkuknow.co.uk***
- Childnet: ***www.childnet.com***
- Kidsmart***: www.kidsmart.org.uk***

Appendix G - Creating strong passwords

(http://www.microsoft.com/protect/fraud/passwords/create.aspx)

Strong passwords are important protections to help you have safer online transactions.

Keys to password strength: length and complexity

An ideal password is long and has letters, punctuation, symbols, and numbers.

- Whenever possible, use at least 14 characters or more.
- The greater the variety of characters in your password, the better.
- Use the entire keyboard, not just the letters and characters you use or see most often.

Create a strong password you can remember

There are many ways to create a long, complex password. Here is one way that may make remembering it easier:

What to do	Suggestion	Example
Start with a sentence or two (about 10 words total).	Think of something meaningful to you.	Long and complex passwords are safest. I keep mine secret. (10 words)
Turn your sentences into a row of letters.	Use the first letter of each word.	lacpasikms (10 characters)
Add complexity.	Make only the letters in the first half of the alphabet uppercase.	lACpAsIKMs (10 characters)
Add length with numbers.	Put two numbers that are meaningful to you between the two sentences.	lACpAs56IKMs (12 characters)
Add length with punctuation.	Put a punctuation mark at the beginning.	?lACpAs56IKMs (13 characters)
Add length with symbols.	Put a symbol at the end.	?lACpAs56IKMs" (14 characters)

Test your password with a password checker

A password checker evaluates your password's strength automatically. (One here - http://bit.ly/1F3MKA)

Protect your passwords from prying eyes

- **The easiest way to "remember" passwords is to write them down.**
  It is okay to write passwords down, but keep them secure. See 5 tips to keep your passwords secret. (http://bit.ly/8VOD73)

Common password pitfalls to avoid

Cyber criminals use sophisticated tools that can rapidly decipher passwords.

Avoid creating passwords using:

- **Dictionary words in any language.**
  Words in all languages are vulnerable.

- **Words spelled backwards, common misspellings, and abbreviations.**
  Words in all languages are vulnerable.

- **Sequences or repeated characters.**
  Examples: 12345678, 222222, abcdefg, or adjacent letters on your keyboard (qwerty).

- **Personal information.**
  Your name, birthday, driver's license, passport number, or similar information.