# E-Safety

# Policy

Reviewed on: Autumn 2016
To be reviewed: Autumn 2017

# St George's CEP School
# Wrotham
# Kent

Signed by: Mrs S Chapman Position held: Chair of Worship, Inclusion & Safeguarding

Signed by: Mr D Jones Position held: Headteacher

# E-Safety Policy

## Who will write and review the policy?

Our e–Safety Policy has been written by the school, building on the KCC e–Safety Policy and government guidance.

The school will appoint an e-Safety Coordinator. They will work closely with the Designated Child Protection Coordinator.

The e-Safety Policy and its implementation will be reviewed annually.

Our School Policy has been agreed by the Senior Leadership Team and approved by governors and other stakeholders such as the PTA.

The School has appointed a member of the Governing Body to take lead responsibility for e-Safety

## 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 part of the statutory curriculum and a necessary 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

## How does Internet use benefit education?

Educational and cultural exchanges between pupils world-wide;

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;

Improved access to technical support including remote management of networks and automatic system updates;

It allows access to learning, wherever and whenever convenient.

Exchange of curriculum and administration data with KCC and DfE;

Access to world-wide educational resources including museums and art galleries;

## How can Internet use enhance learning?

The school Internet access will be designed to enhance and extend education.

Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Staff should guide pupils to 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 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.

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.

Pupils will use age-appropriate tools to research Internet content.

## How will information systems security be maintained?

Virus protection will be updated regularly.

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

Personal data sent over the Internet or taken off site will be encrypted.

Unapproved software will not be allowed in pupils' work areas or attached to email.

Files held on the school's network will be regularly checked.

The computing co-ordinator / network manager will review system capacity regularly.

The use of user logins and passwords to access the school network will be enforced.

Children will not be allowed to bring in external drives/memory sticks from home to use in school.

## How will e-mail be managed?

Schools may have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.

Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.

Staff should not use personal email accounts during school hours or for professional purposes.

Pupils may only use approved email accounts for school purposes.

Pupils must immediately tell a designated member of staff if they receive offensive email.

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

## 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 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.

## Can pupil's images or work be published ?

Images or videos that include pupils will be selected carefully and will not provide material that could be reused.

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 images/videos of pupils are electronically published.

Pupils work can only be published with their permission or their parents/carers.

Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

The School will have a policy regarding the use of photographic images of children which outlines policies and procedures.

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

The school will control access to social media and 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 email addresses, full names of friends/family, specific interests and clubs etc.

Pupils will be advised on security and privacy online and will be encouraged to set passwords, 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.

Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.

Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

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.

Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

## How will filtering be managed?

The school will work with KCC and the Schools Broadband team to ensure that filtering policy is continually reviewed.

The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure. (see appendix 1)

If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.

Any material that the school believes is illegal must be reported to appropriate agencies such as Kent Police, the IWF or CEOP.

The school's broadband access will include filtering appropriate to the age and maturity of pupils.

The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.

Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.

## How will videoconferencing be managed?

Pupils will ask permission from a teacher before making or answering a videoconference call

## The equipment and network

All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

## Users

Parents and carers consent should be obtained prior to children taking part in videoconferences.

Only key administrators should be given access to videoconferencing administration areas or remote control pages.

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

## Content

Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

Videoconferencing will be supervised appropriately for the pupils' age and ability.

## How can 'emerging' technologies be managed?

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

Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use or Mobile Phone Policy.

## How should personal data be protected?

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

## How will Internet access be authorised?

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

All staff will read and sign the 'Staff Information Systems Code of Conduct' or School Acceptable Use Policy before using any school ICT resources.

At Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online material s*(see additional list within the policy).*

Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.

Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.

All visitor to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy.

When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

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 *(see additional list within the policy).*

## How will risks be assessed?

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.

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 Kent Police.

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

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. Neither the school nor KCC can accept liability for the material accessed, or any consequences resulting from Internet use.

## How will the school respond 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 discipline/behaviour policy 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 Children's Safeguard Team or e-Safety officer 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 Area Children's Officer or the County e-Safety Officer.

If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer to communicate to other school in Kent.

**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 will 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 the school to resolve issues.

Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.

Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.

All e–Safety complaints and incidents will be recorded by the school, including any actions taken.

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.

All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

## 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.

The school will provide appropriate levels of supervision for students whilst using the internet and technology on the school site

The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

## How will Cyberbullying be managed?

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 policy on anti-bullying and behaviour.

There are clear procedures in place to support anyone in the school community affected by cyberbullying.

All incidents of cyberbullying reported to the school will be recorded.

Sanctions for those involved in cyberbullying may include: a) The bully will be asked to remove any material deemed to be inappropriate; b) A service provider may be contacted to remove content if the bully refuses or is unable to delete content; c) Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy; d) Parent/carers of pupils will be informed; e) The Police will be contacted if a criminal offence is suspected.

There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.

Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

## How will Learning Platforms and Learning Environments be managed?

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 and staff community will have access to the LP.

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

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.

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

## How will mobile phones and personal devices be managed?

The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school Acceptable Use or Mobile Phone Policies.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.

School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

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.

If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.

If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.

Staff will be issued with a school phone where contact with pupils or parents/carers is required.

Members of staff are advised that personal mobile phones and devices must be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.

Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

If a member of staff breaches the school policy then disciplinary action may be taken.

## **How will the policy be introduced to pupils?**

E-Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.

An e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.

Pupil instruction regarding responsible and safe use will precede Internet access.

An e–Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.

All users 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.

Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

## How will the policy be discussed with staff ?

The e–Safety Policy will be formally provided to and discussed with all members of staff.

Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

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.

To protect all staff and pupils, the school will implement Acceptable Use Policies.

The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.

All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

## 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.

Interested parents will be referred to relevant organisations

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.

Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.

Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.

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

Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.

**Classroom tools and search engines**

No search engine is ever completely safe and appropriate supervision, pre-checks and risk assessments should always be carried out by staff prior to use in the classroom.

- **CBBC Safe search** – child-friendly search engine for primary schools (only searches approved BBC content)
- **Quintura Kids** - search engine for the classroom
- **nICE for Primary Schools** - search engine and library
- **Kids Rex** - search engine
- **Primary School ICT** - video, picture and website search engine
- **VADS** - online resource for searching visual arts
- **NEN image gallery** - for images to use in the classroom
- **Pics4Learning** - for images to use in the classroom
- **Dorling Kindersley Clipart** - clipart for classroom use
- **BBC Schools** - teacher resouces, student activities and bitesize learning
- **Edmodo** - connects learners with people and resources (KS2/3/4)
- **TeacherTube** - video sharing website
- **Schools Tube** - video sharing website
- **Edublogs** - blogging in schools (KS2/3/4)
- **Elgg** - open source social networking tool (KS3/4)
- **Makewav.es** - video blogging and podcasting for schools (KS1/2/3/4)
- **Easywhois** - useful website to check who registered/owns a website (KS3/4)

If schools decide to use search engine sites such as Google or Bing with pupils then they must ensure safe search filtering tools are applied. Schools must be be aware that this only reduces (not removes) the possibility of accessing inappropriate content either accidentally or

otherwise. Therefore, the school must ensure that necessary processes are in place to respond to any filtering breaches. This would include policies and procedures for reporting unsuitable content (for pupils and staff), appropriate supervision and pre-checking of search terms, as well as education for pupils about safe searching and online reliability prior to use.

## E-Safety curriculum materials - teaching about online safety

### General e-Safety Resources

- **ThinkUKnow** - material from Child Exploitation and Online Protection Centre (CEOP) aimed at children aged 4 to 16 (KS1/2/3/4)
- **Childnet International** Smartie the Penguin, Digi
- **Smartie the Penguin** (EYFS/KS1)
- **Digi Duck's Big Decision** (EYFS/KS1)
- **Know it all for Primary Schools**
- **Know it all for Secondary Schools**
- **Kidsmart** (KS2/3)
- **Digital Literacy Scheme of Work** - Foundation Stage to KS4/5
- UK **Safer Internet** Centre - advice and resources for education professionals including a Facebook checklist
- **EE Digital Living** - cyberbullying and keeping children safe resources (KS3/4)
- Create a Budd:e - **primary tool** and **secondary tool** teaching about online risks and consequences (use the demo version to avoid registering) (KS2/3)
- **Welcome to the Web** (KS2/3)
- **Ideas to Inspire** teaching internet safety
- **Teaching Ideas Theme: Staying Safe** (KS1/2)
- **CBBC Stay Safe** - games, videos and activities (KS1/2)
- Newsround: **Caught in the Web** (KS2) Newsround special about staying safe on the internet
- **Webwise** - (KS2/3)
- **Keep Safe** - (KS1/2/3/4)
- **Netsmartz** - (KS1/2/3/4)
- **Get Netwise** - (KS2/3/4)
- **SafetyLand** - internet safety for a young audience (KS2)
- Webonauts - internet academy for **children** and for **parents and educators** (KS1/2)
- **Safe Online Surfing (SOS)** - FBI (KS1/2/3/4)
- **The Web We Want** - handbook for students (KS4/5)
- **Share Take Care** (BBC) - game about online privacy ( KS3/4/5)
- **"In Real Life"** - deals with privacy, sexting, adult content and privacy (KS4/5)

### Cyberbullying

- Newsround: **Bullying: Whose Side are you on?** (KS2)
- **Digizen** (KS3/4)
- **Beat Bullying** (KS2/3/4)
- **Let's fight it together**(KS3/4)

## Gaming

- **It's only a game** (KS2)

## Mobile Phone Safety

- **Phone Brain** (KS3/4) mobile use and phone-paid services

## Social Media

- **Safe** - for primary schools focusing on safer social networking scheme for children. Supported by Digital Me, Radiowaves and Childnet. (KS2/3)
- **Facebook for Educators** - information for staff about facebook and how to incorporate it into your e-safety lessons
- BBC - **a Twitter users guide to the law** - teaching the legal consequences of posting on social media

## Reliability , Privacy and Trust

- **All About Explorers** - evaluate reliability of online information (KS2/3)
- **Information Commissioners Office** - internet safety guidance for young people (KS3/4)
- **The Watchers** - privacy game (on and offline) - (KS2/3)
- **Hoax sites** to test website evaluations (KS2/3/4)

## Piracy and Copyright

- **ProMusic** - exploring piracy and getting music on the internet with students (KS3/4)
- **Copyrights and wrongs** (KS3/4)

## Sex Education and Relationships

- **That's Not Cool** - advice on digital relationships (KS3/4)
- **This is abuse** (KS4/5)
- **Pleasure vs Profit**
- **Sex Education Forum**

## "Sexting"

- Cybersmart - **Tagged**: focuses on cyberbullying and sexting (KS4/5)
- **Sexting resources** from UKSIC (KS4/5)

- **Sexting and the law** - Childnet blog
- **"Picture this"** (KS4/5)
- **Spirito** (KS2/3/4/5)

## Special Educational Needs

- **Munch, Poke, Ping** - guidance for adults working with vulnerable young people (including those in PRUs). Covers mobiles, digital footprints, gaming, sexting.
- **East Midlands E-Safety project** - e-safety for SEN
- **Childnet Star resources for ASD**
- **Know it all for SEN**
- **www.netsmartz.org/SpecialNeeds**
- **www.cybersmart.gov.au/Schools/Teacher resources/Cybersmart Access.aspx**

Formulated by: Mrs L West