The Cottesloe School

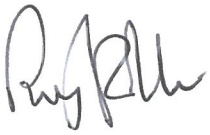
E-Safety Policy

Recommended by:

Resources & People Committee: **Date: 15 October 2015**

Adopted at Full Governing Body Meeting **Date: 24 November 2015**

Signed by R J Collis DL, Chair of Governors:



Review date: Autumn Term 2018 (earlier if any legislative change)

30 November 2015

Please sign and return this form as soon as possible, and keep the attached document for future reference

To: Mr A McBurnie, Headteacher

I confirm that I have received a copy of the E-Safety Policy, which was adopted by the Full Governing Body on 24 November 2015.

Signed ……

Name ……
(Block Capitals)

Date ……

E-SAFETY POLICY – SEPTEMBER 2015

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The School's E-Safety Policy will operate in conjunction with other policies including those for:

- Behaviour Management
- Anti-Bullying
- Child Protection
- Computer Resources for Students and Staff
- Privacy Notice

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.

- Sound implementation of the e-Safety Policy in both administration and curriculum, including secure School network design and use.

- Safe and secure broadband service including the effective management of web filtering.

- National Education Network standards and specifications.

The Cottesloe School acknowledges the assistance of BucksGfl in providing content in this document.

September 2015

E-Safety Audit – Secondary

This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place.

Has the School an e-Safety Policy that complies with BCC guidance?	**Y / N**
Date of latest update: *October 2015*	
The Policy was agreed by governors on: *24 November 2015*	
The Policy is available for staff at: *T:\Policies and Procedures*	
And for parents at: *The Cottesloe School website*	
The Designated Child Protection Coordinator is: *Mrs Chloe Hankin*	
The E-Safety Coordinator is: *Mrs Chloe Hankin*	
Has E-Safety training been provided for both students and staff?	**Y / N**
Do all staff sign an ICT Code of Conduct on appointment?	**Y / N**
Do parents sign and return an agreement that their child will comply with the School E-Safety Rules?	**Y / N**
Have School E-Safety Rules been set for students?	**Y / N**
Are these Rules displayed in all rooms with computers?	**Y / N**
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access.	**Y / N**
Has the School filtering Policy has been approved by SMT?	**Y / N**
Has an ICT security audit has been initiated by SMT, possibly using external expertise?	**Y / N**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Y / N**
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SMT?	**Y / N**
Have appropriate members of staff attended training on the filtering system?	**Y / N**

1. Naturally policy must be translated into practice to protect students and educate them in responsible ICT use.

1.1 Implementing and reviewing the E-Safety Policy

- The E-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, Anti -bullying and for Child Protection.
- The Cottesloe School has appointed an E-Safety coordinator who is the Deputy Safeguarding Lead as the roles overlap.
- Our E-Safety Policy has been written by the School, building on Bucks County Council E-Safety Policy and government guidance. It has been agreed by senior management and approved by Governors.
- The E-Safety Policy and its implementation will be reviewed every three years.
- The E-Safety Policy was revised by: Chloe Hankin (Deputy Safeguarding Lead).

1.2 What does electronic communication include?

- Internet collaboration tools: social networking sites and web-logs (blogs);
- Internet research: websites, search engines and web browsers;
- Mobile phones, tablets and smart watches;
- Internet communications: e-mail and IM;
- Webcams and videoconferencing;
- Wireless or wired games consoles.
- **What are the risks?**

- Receiving inappropriate content;
- Predation and grooming;
- Requests for personal information;
- Viewing 'incitement' sites;
- Bullying and threats;
- Identity theft;
- Publishing inappropriate content;
- Online gambling;
- Misuse of computer systems;
- Publishing personal information;
- Hacking and security breaches;
- Corruption or misuse of data.

2. Teaching and learning

2.1 Why internet use is important

- The purpose of internet use in School is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the School's Management information and administration systems.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- It is an essential element in 21st century life for education, business and social interaction.
- Access to the internet is an entitlement for students who show a responsible and mature approach to its use. Our School has a duty to provide students with quality internet access
- Students will use the internet both in and outside of School and will need to learn how to evaluate internet information and to take care of their own safety and security.

2.2 How Internet use benefit education?

Benefits of using the internet in education include:

- access to learning wherever and whenever convenient;
- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK Schools;
- educational and cultural exchanges between students world-wide;
- access to experts in many fields for students and staff;
- professional development for staff through access to national developments, educational; materials and effective curriculum practice;
- collaboration across 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 Bucks County Council and Department for Education;
- access to learning wherever and whenever convenient.

2.3 Internet use will enhance learning

- The School internet access will be designed expressly for student use and will include filtering appropriate to the age of students.
- Students will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of students.
- Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.4 Students will be taught how to evaluate internet content

- The School should ensure that the use of internet derived materials by staff and by students complies with copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.
- The evaluation of on-line materials is a part of every subject.

3. Managing Information Systems

3.1 Information system security

- The security of the School information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Bucks County Council advisors.
- Personal data sent over the internet will be encrypted or otherwise secured.
- Portable media may not be used without specific permission followed by a virus check.
- Unapproved system utilities and executable files will not be allowed in students work areas or attached to e-mail.
- Files held on the Schools network will be regularly checked.
- The ICT Technician / Network Manager will review system capacity regularly.
- Staff memory sticks will need to be encrypted to ensure that school and student data is protected at all times.

3.2 E-mail

- Students may only use approved e-mail accounts on the School system.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in School to external personal e-mail accounts will be blocked.
- E-mail sent to an external organisation should be written carefully and staff should adhere to guidance in the professional behaviour policy.
- The forwarding of chain letters is not permitted.

3.3 Published content and the School website

- The contact details on the website should be the School address, e-mail and telephone number. Staff or students personal information will not be published.
- Email addresses should be published carefully, to avoid spam harvesting.
- The Headteacher 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.
- The copyright of all material will be held by the School, or be attributed to the owner where permission to reproduce has been obtained.

3.4 Publishing students' images and work

- Photographs that include students will be selected carefully and any student whose photos are used will need to have parents' permission for these to be published.
- Students' full names will not be used anywhere on the Website or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the School Website.
- Work can only be published with the permission of the student and parents.

3.5 Social networking and personal publishing

- The Cottesloe School will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, School attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Students should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or School.
- Teachers' official blogs or wikis should be password protected and run from the School website. Teachers should be advised not to run social network spaces for student use on a personal basis.
- Students should be advised not to publish specific and detailed private thoughts.
- The Cottesloe School is aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.
- Staff that have any social networking sites shouldn't have any links connecting them to The Cottesloe School visible on their page(s)
- School maintained Twitter accounts will be monitored on a regular basis and can be viewed through the school website.

- Staff are strongly advised not to have any social networking accounts, however those that choose to have one must ensure that their security settings are set to the highest available.

3.6 Managing filtering

- The Cottesloe School will work in partnership with external agencies to ensure systems to protect students are reviewed regularly.
- If staff or students discover an unsuitable site, it must be reported to the E-Safety Coordinator or the Network Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the School believes to be illegal must be reported to appropriate agencies such as CEOP (addresses later).
- The School's filtering strategy will be designed by educators to suit the age and curriculum requirements of the students, advised by BucksGfL.
- The staff have access to appropriate software on the School network which allows monitoring and filtering within individual classrooms.

3.6.1 Contact with violent extremists

Many extremist groups such as far right groups, animal rights activists and Islamic fundamentalists who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances some young people may be susceptible to these influences. Bucks LA provides interventions under the Channel project which is part of the Government's Prevent Strategy to divert young people away from extremism.

Staff need to be aware of those young people who are being targeted by or exposed to harmful influences from violent extremists via the internet. Young people should be warned of the risks of becoming involved in such groups. The school will ensure that adequate filtering is in place, with a review of filtering taking place whenever there is any incident of a young person accessing websites advocating violent extremism.

The E-Safety Co-ordinator, along with the ICT Technician, should record and review all incidents in order to establish whether there are any patterns of extremist groups targeting young people. If there is evidence that a young person is becoming deeply enmeshed in the extremist narrative, staff will seek advice from Bucks Prevent Officer to prevent radicalisation.

3.7 Managing videoconferencing

The equipment and network

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- All videoconferencing equipment in the classroom must be switched off when not in use.
- Equipment connected to the educational broadband network should use the 'Adobe Connect' system or the national E.164 numbering system and display their H.323 ID name.
- The equipment must be secure and if necessary locked away when not in use.
- External IP addresses should not be made available to other sites.
- Videoconferencing contact information should not be put on the School Website.
- School videoconferencing equipment should not be taken off School premises without permission. Use over the non-educational network cannot be monitored or controlled.

Users

- Students should ask permission from the supervising teacher before making or answering a videoconference call
- Videoconferencing should be supervised appropriately for the students' age.

- Parental permission will be sought for children to take part in videoconferences.
- Only key administrators should be given access to the videoconferencing system, web or other remote control page.
- Responsibility for the use of the videoconferencing equipment outside School time needs to be established with care.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.
- Recorded material shall be stored securely.
- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Videoconferencing is a challenging activity with a wide range of learning benefits.
- Preparation and evaluation are essential to the whole activity.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non School site it is important to check that the material being delivered is appropriate for the students.

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.
- Mobile phones will not be used during lessons or formal School time and must be switched off whilst in School.
- The sending of abusive or inappropriate text messages is forbidden as is the videoing or photographing of others without permission.
- Staff will be issued with a School phone where contact with students is required, for example on School trips.
- Wireless network will not be available to students for mobile use.
- Sixth Form, some SEN students and staff can use their own laptop to access the School internet. Access is only available via the network manager once a virus check has taken place. Once accessed the user is still bound by the access restrictions as per the School network.

3.9 VLE

- The Schools VLE (virtual learning environment) is monitored on a regular basis by the IT Systems team.
- The VLE has direct links to the CEOP website in order for bad practice to be reported.
- The VLE has a direct link to the thinkuknow website which contains information on internet safety and safe surfing for both students and parents.
- Students are taught about the safe use of the VLE during their ICT lessons.
- The instant messaging service has been removed and is no longer used.

3.10 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

- All staff must read and sign (accept) the 'Computer Resources Staff Code of Practice' before using any School ICT resource.
- The School will maintain a current record of all staff and students who are granted access to School ICT systems.
- Students must apply for Internet access individually by agreeing to comply with the 'Computer Resources Students Code of Practice'.
- Parents will be asked to sign and return a consent form for student access.
- Parents will be informed that students will be provided with supervised internet access.

4.2 Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and linked nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a School computer. Neither the School nor Bucks County Council can accept liability for the material accessed, or any consequences resulting from internet use.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Headteacher will ensure that the E-Safety Policy is implemented and compliance with the Policy monitored.
- The School should audit ICT use to establish if the E-Safety Policy is adequate and that the implementation of the E-Safety Policy is appropriate.
- Methods to identify, assess and minimise risks will be reviewed regularly.

4.3 Handling E-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher, if it is against the Headteacher then the Chair of Governors must be informed.
- Complaints of a child protection nature must be dealt with in accordance with School child protection procedures.
- Students and parents will be informed of the complaints procedure via the School website.
- Parents and students will need to work in partnership with staff to resolve issues.
- As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- Sanctions within the School Discipline Policy include:
  - interview/counselling by Head of Year;
  - informing parents or carers;
  - removal of Internet or computer access for a period of time.

4.4 Community use of the Internet

- 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 students outside of School, e.g. social networking sites.

5. Communication of the Policy

5.1 Introducing the E-Safety Policy to Students

- E-Safety posters will be displayed in all rooms with computers.
- Students 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.
- Instruction in responsible and safe use should precede Internet access.

- An E-Safety module will be included in the PSHCE, Citizenship or ICT programmes covering both School and home use.

5.2 Staff and the E-Safety Policy

- All staff will be given the School E-Safety Policy and its importance explained.
- 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 senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible internet use and on the School E-Safety Policy will be provided as required.

5.3 Enlisting parents' support

- Parents' attention will be drawn to the School E-Safety Policy in newsletters and on the School Website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations listed in Section 6 'E-Safety contacts and references'.

6. E-Safety Contacts and References

BucksICT Support Team Website
http://www.bucksict.org.uk

BucksGfL Website
http://www.bucksgfl.org.uk

Childline
http://www.childline.org.uk/

Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk

Grid Club and the Cyber Cafe
http://www.gridclub.com

Internet Watch Foundation
http://www.iwf.org.uk/

Internet Safety Zone
http://www.internetsafetyzone.com/

Kidsmart
http://www.kidsmart.org.uk/

NCH – The Children's Charity
http://www.nch.org.uk/information/index.php?i=209

NSPCC
http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm

Think U Know website
http://www.thinkuknow.co.uk/

Virtual Global Taskforce – Report Abuse
http://www.virtualglobaltaskforce.com/

7. Acknowledgements

This E-Safety guidance is based in part on the publication "Schools E-Safety Policy 2007" by Kent County Council and we gratefully acknowledge their permission to use it in the production of this document.

8. Review

This policy will be reviewed in three years (earlier if any legislative change).

September 2015

E-Safety Rules

These E-Safety Rules help to protect students and the School by describing acceptable and unacceptable computer use.

- The Cottesloe School owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the School.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The School ICT systems may not be used for private purposes, unless the Headteacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- The use of proxy sites is strictly prohibited.

The School may exercise its right to monitor the use of the School's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the School's computer 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.

Edit this poster for display near computers.

THE COTTESLOE SCHOOL
E-Safety Rules

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

Student:	***Form:***

Student'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 student 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 students 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

Response to an incident of concern

How do we respond?
The flowchart below illustrates an approach to investigating such an incident.