St Christopher's School

A Brighton College School

E-Safety Policy

This policy applies to EYFS

ICT IN THE CURRICULUM

Technology is transforming the entire process of teaching and learning at St Christopher's School. It is a crucial component of every academic subject, and is also taught as a subject in its own right. All of our classrooms are now equipped with electronic whiteboards, projectors and computers. We have an ICT suite in the school, as well as a dedicated suite of computers in the music room.

All of our pupils are taught how to research on the Internet and to evaluate sources. They are educated in the importance of evaluating the intellectual integrity of different sites and why some apparently authoritative sites need to be treated with caution. Some sites that appear to be serious, impartial, historical sites, actually masquerade as sources of racist, homophobic or other offensive propaganda. Some free, on-line encyclopaedias do not evaluate or screen the material posted on them.

THE ROLE OF TECHNOLOGY IN OUR PUPILS' LIVES

Technology plays an enormously important part in the lives of all young people. Sophisticated games consoles, or PSPs (play stations portable), like Wii and Nintendo DS, together with Bluetooth-enabled mobile phones provide unlimited access to the Internet, to SMS messages, to blogging (web logging) services (like Twitter), to skype (video calls, via web cameras built into computers, phones and PSPs), to wikis (collaborative web pages), chat rooms social networking sites (such as Bebo, Facebook, SnapChat, Instagram, What'sApp and MySpace) and video sharing sites (such as YouTube). This communications revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of our role at St Christopher's to teach our pupils how to stay safe in the online environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment.

ROLE OF OUR TECHNICAL STAFF

With the explosion of recent technology, we recognise that blocking and barring sites is no longer adequate. We need to teach all of our pupils to understand why they need to behave responsibly if they are to protect themselves. This aspect is a role for the Head of ICT and other ICT teachers. Our technical support staff play a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of our hardware system, our data and for training our teaching and administrative staff in the use of ICT. They monitor the use of the Internet and emails and will report inappropriate usage to the Head of ICT, who will keep the Headmaster informed.

ROLE OF OUR DESIGNATED SAFEGUARDING LEAD

We recognise that Internet safety is a child protection and general safeguarding issue. *Bridget Laatz* is the school's Designated Safeguarding Lead, supported by *Jude Richards* (Deputy DSL) and *Andrea Bentham*. The ICT Handbook promotes a culture of responsible use of technology, which is consistent with the ethos of our school. All of the staff with pastoral responsibilities have also received training in e-safety issues and the Head of ICT has also received Child Exploitation and Online Protection (CEOP) training. Strong links between the school's comprehensive PSHEE programme and the ICT department ensure that all year groups in the school are educated in the risks and reasons why they need to behave responsibly online. The DSL and Deputy DSL are trained in E-Safety issues and made aware must be made aware of any issues arising involving:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying.

MISUSE – A STATEMENT OF POLICY

At St Christopher's School we will not tolerate the downloading of any illegal material and the Designated Safeguarding Lead will always report illegal activity to the police and/or the Local Child Safeguarding Board (LCSB). If we discover that a child or young person is at risk as a consequence of online activity, the Designated Safeguarding Lead may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). The Designated Safeguarding Lead will handle all allegations of misuse of the Internet. The Headmaster may impose a range of sanctions on any pupil who misuses technology in order to bully, harass or abuse another pupil in line with our Anti-bullying Policy.

INVOLVEMENT WITH PARENTS AND GUARDIANS

We seek to work closely with parents and guardians in promoting a culture of e-safety. We will always contact you if we have any worries about your son or daughter's online behaviour, and we hope that you will feel able to share any worries with us. We recognise that not all parents may feel equipped to protect their son or daughter when they use electronic equipment at home. We therefore aim to arrange discussion evenings for parents where a specialist can advise about the potential hazards of this technology, and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity.

CHARTER FOR THE SAFE USE OF THE INTERNET AND ELECTRONIC DEVICES

"Children and young people need to be empowered to keep themselves safe. This isn't just about a top-down approach. Children will be children - pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends; but we also teach children how to swim." Dr Tanya Byron "Safer Children in a digital world: the report of the Byron Review".

E-safety is a whole-school responsibility and at St Christopher's School the staff and pupils have adopted the following Charter for the safe use of the Internet at school:

Cyberbullying

- Cyberbullying is a particularly pernicious form of bullying as it can be so pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. Our school's Anti-bullying Policy describes the preventative measures and procedures that will be followed when we discover cases of bullying.
- Proper supervision of pupils plays an important part in creating a safe ICT environment at school, but everyone needs to learn how to stay safe outside school.
- We value all of our pupils equally. It is part of the ethos of St Christopher's School to promote considerate behaviour and to value diversity.
- Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and he or she should not be afraid to come forward.

Treating Other Users with Respect

- We expect pupils to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face-to-face contact. Pupils should always follow the school's Code of Conduct.
- Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. Our Anti-bullying Policy available on our website and from the school office. The school is strongly committed to promoting equal opportunities for all, regardless of race, gender, gender orientation or physical disability.
- All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or worrying issue to a member of the pastoral staff.

Keeping the School Network Safe

- We adhere to the BECTA guidelines regarding E-teaching and the Internet.

- Certain sites are blocked by our filtering system and our ICT Department monitors pupils' use of the network.
- We issue all pupils in the Middle and Upper School with their own personal school login, which is password-protected. We give guidance on the reasons for always logging off and for keeping all passwords securely.
- Pupils in III Form and above are introduced to safe and secure e-mailing through think.com, which is password protected, teacher monitored and includes no advertising.
- Access to sites such as *Hotmail* is not allowed on the school's network.
- Pupils are not allowed to access the internet or the ICT suite if they are not supervised by a member of staff.
- We have strong anti-virus protection on our network, which is operated by the ICT Department.
- Any member of staff or pupil, who wishes to connect a removable device to the school's network is asked to arrange in advance with the ICT Department to check it for viruses.

Promoting Safe Use of Technology

The school will arrange annual Safe Internet Days. Pupils of all ages are encouraged to make use of the excellent online resources that are available from sites such as:

- Childnet International (www.childnet-int.org)
- Digizen (www.digizen.org.uk)
- Cyber Mentors (www.cybermentors.org.uk)
- Cyberbullying (www.cyberbullying.org)
- E-Victims (www.e-victims.org)
- Bullying UK (www.bullying.co.uk)

Pupils often prepare their own models of good practice, which form the subject of presentations at assemblies. They cover the different hazards on the Internet, such as grooming, stalking, abuse, bullying, harassment and identity theft. Guidance covers topics such as saving yourself from future embarrassment, explaining that any blog or photograph posted onto the Internet is there permanently. Anything that has been deleted may be cached in a search engine, company server or Internet archive and cause embarrassment years later.

Safe Use of Personal Electronic Equipment

- Our guidance is that no one should put anything onto the web that they would not say to their grandmother!
- We offer guidance on the safe use of social networking sites and cyberbullying, which covers blocking and removing contacts from "buddy lists".

- Our lessons include guidance on how pupils can identify the signs of a Cyber- stalker, and what they should do if they are worried about being harassed or stalked online.
- We offer guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe. Privacy is essential in the e-world.
- We give guidance on how to keep safe at home, by encrypting your home wireless network, not opening unknown attachments and reporting any illegal content. Similarly we cover how a mobile phone filter can be activated, and how to block nuisance callers.
- We advise on the responsible use of skype.

<u>Considerate Use of Electronic Equipment</u>

- Only children in the Upper School (Years 7 and 8) may carry mobile phones; these devices should be handed in to the school office upon arrival and collected at the end of the day. The Headmaster may confiscate phones if they are not handed in to the school office.

- Sanctions may be imposed on pupils who use their electronic equipment without consideration for others.

We expect all pupils to adhere to this charter for the safe use of the Internet. Copies are given to all pupils and their parents, and we may impose sanctions for the misuse, or attempted misuse of the internet, mobile phones and other electronic devices.

RESPONSIBLE INTERNET AND ELECTRONIC MAIL USE

The rules listed below, and the ICT Contacts, refer to the documents above and are designed to ensure that pupils use ICT facilities in a sensible, proper and safe manner.

Network Etiquette

Network users are expected to abide by the generally accepted rules of network etiquettes. These rules include (but are not limited to) the following:

- I will always be polite and use appropriate language
- I will show consideration and respect for others at all times
- I will cite all quotes, references and sources
- I will always think about the social consequences of what I do on the computer

St Christopher's School Responsibilities

1. St Christopher's School reserves the right to install hardware and/or software to monitor the actions of individual users in order to determine whether or not those actions are in compliance with school policy, and with local and national laws.
2. A reasonable level of monitoring of pupil use of installed systems is expected of school employees. The school expects that violations of this policy be reported to the Head of ICT, who will inform the Headmaster.
3. St Christopher's School is not liable for damage to or loss of files due to system malfunction or administrator error.
4. The Network Manager has the right to monitor all accounts for the purpose of insuring that all systems remain operable and optimised for users.
5. The Network Manager, after giving prior notice to all users, will periodically purge inactive files.

Chrome Book Usage

In addition to the school's normal ICT policy, the following main additions apply and have to be agreed to, for any child to be allowed to use a Chromebook in school:

- Pupils must be aware of the consequences of their actions and ensure they use their Chromebook for positive activities. Unpleasantness, cruelty, or any other inappropriate use (as outlined in the Computing Contract) will not be tolerated.

- The school cannot be held responsible for loss, vandalism or damage to any personally owned ICT equipment.

- It is accepted that the school will have access to any child's Chromebook or school user identity and may review the History Log at any time to see what sites have been visited. If an inappropriate site has been visited and/or the Chromebook has been used at unusual times, then parents will be informed and the school will retain the right to withdraw the Chromebook from the child for a period of time.

- If a child does not have a Chromebook the school will obviously endeavour to minimise any resulting disadvantage.

- No other personal laptops, iPads or other such equipment can be brought into school as they will not have our web filtering and security protocols on them.

Last reviewed: September 2016
Next review: September 2018

St Christopher's School E-Safety Contract
Year 1 to 6 pupils

As a pupil at St Christopher's School I will be using a Chromebook/ laptop at school. The following rules apply to this usage:

At all Times

- I will remember the device/s is there as a tool to support my learning – I have a duty to ensure that this is what it is used for.
- I will not attempt to interfere with any of the settings on the device/s
- I will remember everything I have been taught about Internet safety in order to keep myself safe and my personal information secure.

At School

- I will access the system using my own login name and password, which I will keep a secret. I will logout of accounts when leaving a computer/ Chromebook unattended.
- I will not access other people's files or edit, alter or delete their work.
- I will not willfully vandalise or destroy any computer equipment.
- I will not use any devices for games, chat or downloading programs unless authorised by a teacher. Social networking is strictly prohibited.
- I will report any unpleasant material or messages sent to me.
- I understand that the school has the right to check my computer files and communications and has the right to record the Internet locations I visit.
- Emails should not be sent to anyone outside of the school during the school day.
- No emails should be sent during school hours without specific instruction from a teacher.
- If I am unsure about anything I will ask

Violation Consequences

- Teachers may deny, suspend or revoke any network/Internet access as deemed appropriate
- A Level 2 will be given for any misuse, including playing games during lessons or interfering with another pupil's device.
- If behaviour reoccurs, you will be given a detention and you will be banned from using computing equipment at the Head of Section's discretion.
- In extreme circumstances the Headmaster may take disciplinary action, which may include suspension or exclusion, or legal action.

If you are happy with what you have read in the School's E-Safety Contract, please sign below and return a copy to the school.

Child's Name: _____ Form : _____

_____

Pupil signature

_____

Parent signature

_____

Name of Parent (printed)

<u>Notes for Parents to help control electronic device usage for non-educational purposes:</u>

- The Internet at school is strictly controlled – strong filters are in place and Facebook etc. are blocked – but we need your co-operation in monitoring usage at home
- In the same way we can (and do) monitor Chromebook and computer usage at school and ensure that there is plenty of time when your children are not using them, but we need your help with this at home
- Act as role model for your children in your own use of 'smart' mobile devices – switching them off, not using them during meal-times or while talking with children
- Discuss openly the use of electronic devices (both yours and theirs) with your children and help them to abide by their contract
- Talk to your children about being thoughtful and considerate in the wording of e-mails to friends and remind them that the school monitors e-mail usage from their account
- Be prepared to use the draconian measures that may be appropriate but may often cause friction and resentment amongst children, for example, remove the electronic device/s for a certain period of time.

St Christopher's School E-Safety Contract
Year 7 and 8 pupils

As a Year 7 or 8 pupil at St Christopher's School I will be using a Chromebook at school and at home. The following rules apply to this usage:

At all Times

- I will remember the Chromebook is there as a tool to support my learning – I have a duty to ensure that this is what it is used for
- I will not attempt to interfere with any of the settings on my Chromebook
- I will remember everything I have been taught about Internet safety in order to keep myself safe and my personal information secure.
- I will take great care of my Chromebook and never leave it lying around
- I will keep files on my Chromebook organised, and make sure that all work is saved in the correct place (Google Drive)

At School

- I will access the system using my own login name and password, which I will keep a secret. I will logout of accounts when leaving a computer unattended.
- I will not access other people's files or edit, alter or delete their work.
- I will not willfully vandalise or destroy any computer equipment.
- I will not use my Chromebook for games, chat or downloading programs unless authorised by a teacher. Social networking is strictly prohibited.
- I will report any unpleasant material or messages sent to me.
- I understand that the school has the right to check my computer files and communications and has the right to record the Internet locations I visit.
- Emails should not be sent to anyone outside of the school during the school day.
- No emails should be sent during school hours without specific instruction from a teacher.
- I will never use my Chromebook when walking around school
- I will not get my Chromebook out until/unless instructed by the teacher
- I will not use my Chromebook during break times or form period
- If I am unsure about anything I will ask

Out of school

- I will not use my Chromebook during the journey to and from school
- If I do not need my Chromebook when doing school prep I will switch it off or give it to my parents
- I will make sure that I have "no media" time, during which I read a paper book, exercise, pursue a hobby or talk with my family
- I will remember to charge my Chromebook and will bring it to school every day
- I will share what I am doing on my Chromebook with my family.

Violation Consequences

- Teachers may deny, suspend or revoke any network/Internet access as deemed appropriate
- A Level 2 will be given for any misuse, including playing games during lessons or interfering with another pupil's Chromebook.
- If your behaviour reoccurs, you will be given a detention and you will be banned from using a Chromebook at the Head of Section's discretion.
- In extreme circumstances the Headmaster may take disciplinary action, which may include suspension or exclusion, or legal action.

If you are happy with what you have read in the School's E-Safety Contract, please sign below and return a copy to the school.

Child's Name: _____ Form : _____

_____

Pupil signature

_____

Parent signature

_____

Name of Parent (printed)

Notes for Parents to help control Chromebook usage for non-educational purposes:

- The Internet at school is strictly controlled – strong filters are in place and Facebook etc. are blocked – but we need your co-operation in monitoring usage at home

- In the same way we can (and do) monitor Chromebook usage at school and ensure that there is plenty of time when your children are not using them, but we need your help with this at home

- Act as role model for your children in your own use of 'smart' mobile devices – switching them off, not using them during meal-times or while talking with children

- Discuss openly the use of electronic devices (both yours and theirs) with your children and help them to abide by their contract

- Ask your children to show you what they have been using their Chromebook for, both at school and home

- Talk to your children about being thoughtful and considerate in the wording of e-mails to friends and remind them that the school monitors e-mail usage from their account

- Agree a time that you will unplug the broadband router (will stop the Chromebook access to e-mails and internet whilst not preventing off-line use) or limit the amount of airtime they have on their mobile

- Be prepared to use the draconian measures that may be appropriate but may often cause friction and resentment amongst children, for example, remove the Chromebook or other electronic devices.