`St Christopher's School

A Member of the Brighton College Family of Schools

POLICY ON PUPILS' USE OF ICT, MOBILE PHONES AND OTHER ELECTRONIC DEVICES

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 up to the end of year 8. All of our classrooms are now equipped with electronic whiteboards, projectors and computers. We have a mobile ICT facility in the form of 40 Chromebooks. In addition there are 22 laptops in the Maths room which is where all the dedicated Computing lessons in Reception to year 8 are taught. There is also a 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 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 all staff involved in teaching and using ICT and with our increasing cross curricular use of ICT especially in years 4 to 8 the specific teaching of safety when using computers and the issue of Cyber Bullying are best dealt with during dedicated PSHCE sessions as well as a half term unit of study within Computing lessons. Our technical support staff has 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 Computing, who will keep the Headmaster informed.

ROLE OF OUR CHILD PROTECTION OFFICER

We recognise that Internet safety is a child protection and general safeguarding issue. The Deputy Head Pastoral is the school's Child Protection Officer. 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 Computing will receive Child Exploitation and Online Protection (CEOP) training. Strong links between the school's comprehensive PSHCE 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.

MISUSE – A STATEMENT OF POLICY

St Christopher's School we will not tolerate the downloading of any illegal material and the Headmaster 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 Headmaster may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). 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. The Deputy Head Pastoral, who is the school's Child Protection Officer or the Head of Computing, will handle all allegations of misuse of the Internet dependent on its nature and severity.

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 have therefore arranged 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.
- Anyone suffering from this should save upsetting images or messages as these are valuable forms of evidence

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 is 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* or *Facebook* 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.

Personal Chromebooks used in years 7 and 8 have to be added to the St Christopher's platform for them to be used in school and to ensure it is secure.
The advantages of this are;

- **Single sign-in which is their school e-mail account which automatically means they are protected by our web filtering service called Surf Remote when working in school or anywhere else**
- They cannot logon to the device using their own G-Mail account but can access personal e-mail accounts via G-Mail once logged on to the device

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)
- E-Victims (www.e-victims.org)
- Bullying UK (www.bullying.co.uk)

Pupils often prepare their own models of good practice. 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 or allow to be published in a national newspaper.
- We offer guidance on the safe use of social networking sites and cyber bullying, 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.

Considerate Use of Electronic Equipment

- Only children in the Upper School (Years 7 and 8) or a Middle School Pupil (years 4 to 6) in exceptional circumstances 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.

CONTRACT FOR RESPONSIBLE INTERNET AND ELECTRONIC MAIL USE

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

Rights and Responsibilities of Users

- I will access the system using my own login name and password, which I will keep a secret. I will protect my personal and shared accounts from unauthorised use by logging out of all authorised accounts when leaving a computer unattended.
- I will not access other people's files or edit, alter or delete their work. This includes all files and folders in the shared area.
- I will only use the computer for work required for my education.
- I will not wilfully vandalise or destroy any computer equipment including moving, repairing, reconfiguring, modifying, introducing viruses or attaching external devises to existing systems.
- I will not use the facilities for games, chat or downloading programs.
- I will communicate only with people I know, or those whom my teacher has approved.
- To protect myself and other pupils, I will report any unpleasant material or messages sent to me. I understand that this report would be confidential.
- 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.
- I will not waste resources, such as paper or someone else's time when using a computer.
- I will not give my home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given me permission to do so.
- I will always log out of any site I am working on and when using the school laptops ensure that I log off properly and do not shut the laptop until the login screen has reappeared so allowing the next user to be able to sign in

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 Computing, who will inform the Deputy Head Pastoral and 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.

Violation Consequences

In the first instance, the Head of Computing may deny, suspend or revoke any network/Internet access as deemed appropriate; and

In the second instance, the Deputy Head Pastoral and 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 Charter and the Contract, please sign below and return a copy to the school by Friday 14th November 2014

Child's Name: ________________________________ Form: ________________

____

Pupil signature

____

Parent signature

____ Date_________________

Name of Parent (printed)

The above policy is in line with our Child Protection Policy.

Reviewed and Updated Oct 2014 – C Pincott

Updated January 2015 – C Pincott

Review September 2015