The Compton School: E-safety Policy

(Updated November 2015)

Our E-Safety Policy has been written by the school, building on the Barnet Safeguarding Children Board E-Safety Strategy and BECTA guidance.

Introduction

Our policy applies to all students, staff, governors and volunteers associated with the school. The 'staying safe' outcome of Every Child Matters is at the heart of the policy. The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

The are five main areas of this policy:

1. Current digital technologies
2. E-Safety risks
3. Strategies to minimise risks
4. How will complaints regarding E-safety by handled?
5. Staff code of conduct for ICT

1. Current digital technologies

ICT in the 21st century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of children include:

- The internet
- Telephone text messaging
- Instant messaging often using simple web cameras
- Social networking sites (Facebook)
- Video broadcasting sites (Youtube)
- Chat rooms
- Blogs
- Podcasting
- Gaming sites
- Music download sites
- Mobile phones with camera and videos
- Games consoles with internet communication
- Smart phones with e-mail and web functionality
2. E-Safety Risks
The risks can be summarized under the following headings as identified in BECTA’s Safeguarding Children in a Digital World (2006) advice.

2.1 E-Content
Exposure to age inappropriate material – pornography etc.
Exposure to inaccurate or misleading information
Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance.

2.2 E-Contact
Grooming using digital communication, leading to sexual assault.

2.3 E-Commerce
Exposure of minors to inappropriate commercial advertising
Exposure to online gambling
Commercial and financial scams

2.4 E-Culture
Bullying via mobile phones/ social networking/ websites or other forms of digital communication including untruthful, hurtful and abusive comments or imagery intended to denigrate or humiliate another.
Illegal downloading of copyrighted materials i.e. music and films.

3. Strategies to minimize e-safety risks
- E-safety agreement signed by all parents and students.
- All parents to provide consent for publication of photographic images
- All parents to receive a home office booklet called Keep You Child Safe on the internet.
- E-Safety notices in all classrooms
- E-Safety taught to all students through year 7 ICT curriculum
- Guidance on tackling cyber bullying a theme for all year group assemblies supported by posters in all classrooms
- Sanctions for inappropriate use of the internet communicated through assemblies and posters in classrooms
- Log on screen for all students and staff has a tick box indicating acceptance of the school internet policy.
- Filtering systems to prevent access to inappropriate material.
- Use of RMTutor, inclass monitoring of PC use by teachers
- Surveillance software monitoring all PC use within the school.
- Banned item searches to ensure mobile phones are not used within school.
- All staff sign a Computer and Internet Acceptable Use Policy.
- Child protection issues reported to the Associate Headteacher responsible for Child Protection
- E-Safety concerns are reported direct to the Deputy Headteacher responsible for ICT systems.

4. How will complaints regarding E-safety be handled?
The school will take all reasonable precautions to ensure E-Safety. However, owing to the global scale and linked nature of internet content, the wide availability of mobile and digital technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the local authority can accept liability for material accessed, or any consequences of internet access.
Appendix 1.

The Compton School Computer and Internet Acceptable Use Policy
For Staff

All staff having access to the networks must sign a copy of this Computer and Internet Acceptable Use Policy and return it to the School Office.

The computer network is owned by the school and is made available to staff to assist their professional development. This computer and Internet Acceptable Use Policy covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems and has been drawn up to protect everyone.

- I will only use the school’s digital technology resources and systems for Professional purposes or for uses deemed ‘reasonable’ by the Head and Governing Body.
- I will only use the school’s approved, secure email system(s) for any school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / Deputy Head responsible for ICT systems.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I will ensure all documents are saved, accessed and deleted in accordance with the school’s Data Protection procedures.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any ‘loaned’ equipment up-to-date, using the school’s recommended system.
- I will not use personal digital cameras or camera phones for transferring images of pupils or staff without permission.
- I will use the school’s Learning Platform in accordance with school / and London Grid for Learning advice.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely for professional use.
- I will ensure any confidential data that I wish to transport from one location to another is password protected.
I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

I will ensure I am aware of digital safety-guarding procedures so they are appropriately embedded in my classroom practice.

I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

I will report any incidents of concern regarding children's safety to the e-Safety Coordinator, the Designated Child Protection Coordinator or Headteacher.

I will only use LA systems in accordance with any Corporate policies.

**Social Media**

I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role and are secure against access by uninvited users i.e. students both current and former.

I will ensure that no postings on social network sites link the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.

I will not post any images of employees, children or anyone directly connected with the school whilst engaged in school activities.

I will not make share any personal information with a child or young person.

I will ensure that personal social networking sites are set to Private and students are never listed as approved contacts.

I will never use or access social network sites of students.

I will not use web based communication to send personal messages to students.

I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action.

**ALL SCHOOL NETWORK, INTERNET AND MANAGED LEARNING ENVIRONMENT SYSTEMS ARE MONITORED AND WE RESERVE THE RIGHT TO EXAMINE ANY AREA OF THESE SYSTEMS.**

The use of computer systems without permission or for inappropriate purposes could be a criminal offence under the Computer Misuse Act 1990 (The Computer Misuse Act 1990 makes it a criminal offence to “cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer”. Sending malicious or threatening e-mails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the Telecommunications Act (1984).)

**User Signature**
I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school’s most recent Acceptable Use Policy (normally an annual revisit).

I agree to abide by the school’s most recent Acceptable Use Policy.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school’s ICT resources and systems.

Appendix 2.

The Compton School Computer and Internet Acceptable Use Policy
For Students

All students having access to the networks must sign a copy of this Computer and Internet Acceptable Use Policy and return it to the School Office.

The computer network is owned by the school and is made available to students to further their education. The school’s Computer and Internet Acceptable Use Policy has been drawn up to protect everyone and failure to comply with this policy will result in you not being able to use school computers or more serious sanctions in accordance with the ICT Sanctions Triangle

- Students must only access the network and Internet via their authorised account and password. **Students must not make this information available to any other person.**
- Students are only allowed to use the network computers when a member of staff is present.
- The school reserves the right to examine and / or delete any files that may be held on its computer network and / or to monitor any Internet sites visited or e-mails sent or received.
- Users may not install, or attempt to install, their own software; nor may they delete or attempt to delete system software, alter another user’s files.
- Students must not perform a function with the intent to gain unauthorised access to any programs, files or data held on the computer.
- Activity which threatens the integrity of the school ICT systems (‘hacking’), or activity which attacks or corrupts other systems, is forbidden.
- Users must not attempt to repair or rearrange the hardware and any such issues should be referred to the ICT Systems and Network manager.
- The cost of replacement or repair for any damage caused through neglectful or irresponsible behaviour or acts of vandalism or will be charged to the individual concerned.

**All Internet activity must be appropriate to the student’s education.**
- The use of chat rooms and social networking sites is not allowed and appropriate action will be taken.
- Students may not download music files to the school network and the sharing of music files is strictly forbidden.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material are forbidden and appropriate action will be taken.
- Students must not use proxy websites to gain access to banned web material.
- Use of the school’s network for financial gain, gambling, political purposes or advertising is forbidden.
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received. E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.
- Copyright and intellectual property rights must be respected.
- Permission must be asked of if you are taking a photograph or recording an image of someone on school premises (whether teacher, student, volunteer, visitor etc.) and the image may only be used or educational reasons.
- Posting anonymous e-mails and forwarding chain letters is forbidden.
- Students must report any accidental access to, or receipt of inappropriate materials, or filtering breach to the E-learning Co-ordinator.
- Students must only access the Managed Learning Environment (MLE) via their authorised account and password. Students must not make this information available to any other person.
- The MLE is a learning platform and must not be used for social networking.
- Students should use correct English and grammar at all times on the MLE.

ALL SCHOOL NETWORK, INTERNET AND MANAGED LEARNING ENVIRONMENT SYSTEMS ARE MONITORED AND WE RESERVE THE RIGHT TO EXAMINE ANY AREA OF THESE SYSTEMS.

The use of computer systems without permission or for inappropriate purposes could be a criminal offence under the Computer Misuse Act 1990. (The Computer Misuse Act 1990 makes it a criminal offence to “cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer”. Sending malicious or threatening e-mails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the Telecommunications Act (1984).)

I have read and understood the Policy above, and agree to the conditions stated. I understand that my access to the network may be restricted or denied if I knowingly contravene any of these conditions. I have also read and agree to the attached ‘Rules and Responsibilities for Computer and Internet Use’.

Student Print Full Name ….
…………………………………………Signed…………………………Date……...

Parent Print Full Name……
………………………………………… Signed ……………………… Date……...

01/09/12