CITY OF LONDON SCHOOL FOR GIRLS

POLICY ON PUPILS' USE OF IT, MOBILE PHONE AND OTHER ELECTRONIC DEVICES

Policy last reviewed by:	David Libby. Neil Codd, Michael Martyn
Date policy last reviewed:	September 2020
Approved by:	Board of Governors
Date approved:	5th October 2020

Contents

1. IT in the Curriculum

Technology has transformed the entire process of teaching and learning at City of London School for Girls. It is a crucial component of every academic subject. All of our classrooms are equipped with digital screens, projectors and computers. We have a number of computers in school (in the library, Sixth Form work room, C floor corridor) which pupils may use for private study.

All of our pupils are taught how to research on the Internet and to evaluate sources. They are educated into 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, jihadist or other propaganda. Some free, on-line encyclopaedias do not evaluate or screen the material posted on them.

2. The role of technology in our pupils' lives

Technology plays an enormously important part in the lives of all young people. Sophisticated mobile devices provide unlimited access to the internet and services such as instant messaging blogging, video calls e.g. Skype/Facetime, wikis, chat rooms, social networking sites e.g. Facebook, Instagram and Tumblr 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 CLSG to teach our pupils how to stay safe in this 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.

3. Role of our technical staff

With the explosion in 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 our Designated Safeguarding Lead and our pastoral staff. Our technical staff have 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 IT. They monitor the use of the internet and emails and will report inappropriate usage to the pastoral staff.

4. Role of our Designated Safeguarding Lead

We recognise that internet safety is a child protection and general safeguarding issue.

Our Designated Safeguarding Lead (DSL) has been trained in the safety issues involved with the misuse of the internet and other mobile electronic devices. She works closely with the Local Safeguarding Children's Partnership (LSCP) and other agencies in promoting a culture of responsible use of technology that is consistent with the ethos of the school. All of the staff with pastoral responsibilities have also received training in e-safety issues and they are supported by the e-safety coordinator. The school's comprehensive PSHCEE programme on e-safety is the DSL's responsibility in consultation with the eSafety Coordinator and the Heads of Section. She will ensure that all year groups in the school are educated in the risks and the reasons why they need to behave responsibly online. It is her responsibility to handle allegations of misuse of the Internet.

5. Promoting safe use of technology

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)

They prepare their own models of good practice, which form the subject of presentations at assemblies and discussion in the meetings of the School Council. 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.

6. Misuse: Statement of Policy

We will not tolerate any illegal material, and 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, we may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). We will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil or any member of the school community in line with our anti-bullying policy.

7. 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 parents if we have any worries about their daughter's behaviour in this area, and we hope that they will feel able to share any worries with us. We recognise that not all parents and guardians may feel equipped to protect their daughter when they use electronic equipment at home. We have arranged briefings for parents about the potential hazards of this exploding technology, and the practical steps that parents can take to minimise the potential dangers to their daughters without curbing their natural enthusiasm and curiosity, and continue to plan such events, in particular in conjunction with the Friends of CLSG.

8. IT Code of Conduct

The IT Code of Conduct applies to all users of Information Technology (IT) at The City of London School for Girls.

The Philosophy of the school is to allow open access to the IT system but this is only possible if the students behave in a sensible and responsible manner. The school's general code of conduct requires that 'all members of the school community are treated decently and are allowed to get on with their work and other activities in a friendly, tolerant and purposeful atmosphere'. It is important that this concept is applied to the use of the IT system in order to allow the school to develop a cutting edge IT system which will enhance the learning experience of all students at the school.

I will:

- Keep my password safe, change it as necessary and not reveal it to anyone else
- Treat the IT facilities with care and leave the area clean and tidy when finished
- Only use the school's facilities for work related to school such as subject work, homework and course work, except for games at lunchtime
- Print as little as possible to conserve resources
- Use e-mail and public forums sensibly and constructively using good English
- Keep my mobile phone or other personal electronic device switched off and stored securely during the school day. Though I may use them during lunch times. This does not apply to devices issued to students by the school e.g. iPads which should be used as directed by the subject teacher.

I will not:

- Use the IT facilities, a mobile phone or any electronic device to access offensive or unacceptable material (such as pornography, sexist or racist material)

- Use email, blogs, forums or social networking sites whether accessed from a computer, mobile phone or any electronic device connected to the school's network, a mobile phone network or communicating via Bluetooth to send or encourage material which is pornographic, illegal, offensive or annoying or in any way invades another person's privacy
- Publish any comments, images or videos about situations or individuals from the school community on blogs, forums or social networking sites in the Public Domain • Use any part of the school's IT system, a mobile phone or any electronic device to tease or bully another person
- Post anonymous messages or forward chain messages
- Gain, or attempt to gain, unauthorised access to any part of the school's IT system
- Make, or attempt to make unauthorised changes to any computer document or file
- Gain, or attempt to gain, unauthorised access to any other computer system
- Download computer documents/files (including games, video clips, sound) without permission
- Breach copyright regulations
- Deliberately place a virus, malicious code, or other inappropriate program, onto the school computers
- Download software from the Internet (including screen savers, games, video clips, audio clips, *.exe files).

I understand that:

- The school runs auditing software which records inappropriate actions made by the student online or when using software and records all websites visited.
- E-mail is continually monitored and random checks may be made on user areas
- The school may look at any files and data held in user areas
- Use of the computer network, the Internet & email is a privilege which may be withdrawn if abused and further sanctions may follow
- Use of the school's facilities for any unauthorised activity may be a criminal offence under the Computer Misuse Act (1990), will be treated as such by the school, and the appropriate authorities may be notified.
- Staff may confiscate personal equipment that is being used during the school day for periods of up to 5 days.
- Sanctions may be imposed on pupils who use their electronic equipment without consideration for others.

I will never:

- Tell anyone I meet on the Internet my home address, my telephone number or my school's name, unless my teacher specifically gives me permission
- Send anyone my picture without permission from my parents/carer
- Arrange to meet anyone in person without first agreeing it with my parents/carer and get them to come along to the first meeting

- Stay in an Internet chat room if someone says or writes something, which makes me feel uncomfortable or worried, and I will always report it to a teacher or parent
- Respond to unpleasant, suggestive or bullying e-mails or bulletin boards and I will always report it to a teacher or/parent
- Tamper with hardware (including the connecting of personal or unauthorized equipment to the network), software or the work of others.

9. IT Acceptable Use Policy – in School

- The use of any program, including access to the internet, which has not been approved by your teacher, may result in a network or Internet ban.
- Listening to music or streaming media (watching videos) is not allowed unless it is directly related to the class activity and has been approved.
- Changing any of the settings on a computer or any school issued digital device including the logon domain name, cursor or desktop is strictly prohibited.
- Sharing your password/user area with others is unacceptable as is accessing anyone else's user area.
- Signing into a school owned device with a private account or Apple ID is prohibited unless directed to do so by your teacher.
- Eating, drinking and irresponsible behaviour is not permitted in IT rooms under any circumstances.
- Using classroom computers and projectors is prohibited unless expressly authorised by a member of staff.
- Work must be saved using relevant filenames so that you can identify documents at a later date and must not be of an offensive nature. Documents saved with default filenames such as untitled, doc1, doc2 etc. will be deleted automatically without question.
- Work that is no longer required must be deleted.
- All work produced on the school network must be saved in your user area, an appropriate shared area or if authorised by the subject teacher, in the Cloud. Any work that is saved on the local machine or any other unauthorised location may be automatically deleted without warning.
- The downloading or installation of any executable file (exe or dmg on a Mac), game or software is prohibited.
- Faulty equipment should be reported to the class teacher or the IT Systems Manager as soon as possible.
- The use of pen drives is only permitted for storage of work documents, not software such as games & applications. Pen drives must only be used on school computers if you have up-to-date antivirus software on your home computer.
- Laser printers must only be used for printing on to standard paper. You must not use card or transparencies.

- Downloading software of any type whatsoever from the Internet is strictly forbidden as well as the viewing, printing or saving of unsuitable material e.g. pornographic, racist, sexist or otherwise offensive content.
- Attention should be paid to copyright laws when saving documents, sounds, pictures etc. from the Internet, especially when printing and integrating in other work.
- The use of the Internet at The City of London School for Girls is for educational purposes only. Other non-educational use such as text messaging, Instant messaging or chatting is not allowed unless explicitly permitted by the Director of IT.
- If you send email from school then it is your responsibility to ensure that anything you write is sensible, inoffensive, and will not be likely to reflect badly on the school. Emails sent from school are traceable to the originator. Spamming or pranking other computer users will be dealt with severely.
- Your user area and all of your files remain the sole property of The City of London and are subject to inspection at any time.
- These rules have been drawn up with reference to government guidelines on school computer and Internet use, and are not necessarily exhaustive, but explain the kind of behaviour and responsibility that is expected of you in school.
- You should be aware that the Director of IT has the ability to monitor everything that happens on the network. This includes the ability to view the contents of computer screens remotely, log the contents of all web sites and IP addresses contacted by a user including all email sent and received and logging of the time spent by a user on any computer in any part of the school.

Any user breaking these rules will have access to the school network and/or the Internet withdrawn and may well face further action under the Computer Misuse Act 1990. In addition, activities such as publishing inaccurate material relating to a student or a member of staff on the Internet may result in an action being taken in the civil courts for Defamation.