CITY OF LONDON SCHOOL FOR GIRLS

IT & E-SAFETY POLICY

Policy last reviewed by:	Michael Martyn, Rachel Brincat
Date last reviewed:	September 2020
Approved by:	
Date approved:	

Contents

1. Introduction

1.1 The City of London School for Girls recognises that the internet and other digital technologies provide a vast opportunity for children and young people to learn. Unlike any other mode of technology, the internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning. It is essential that this policy is read and used in conjunction with other school policies.

1.2 As part of our commitment to learning and achievement The City of London School for Girls wants to ensure that the internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement.
- Develop the curriculum and make learning exciting and purposeful.
- Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security.

To enable this to happen, we have taken a whole school approach to eSafety which includes the development of policies and practices, the education and training of staff, pupils and parents and the effective use of the School's IT infrastructure and technologies. E-safety is an essential strand of Safeguarding and Child Protection at CLSG.

1.3 The City of London School for Girls as part of this policy, holds steadfastly to the ethos that there should be an equitable learning experience for all pupils using IT technology. We recognise that IT can allow all pupils increased access to the curriculum and other aspects related to learning.

1.4 The City of London School for Girls is committed to ensuring that all its pupils will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are educated as to the dangers that exist so that they can take an active part in safeguarding them.

1.5 The use of these new technologies can put young people at risk within and outside the school. The dangers that they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to, loss of or sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/Internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.

- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

2. Scope of policy

2.1 The policy applies to:

- All pupils
- All teaching and support staff (including peripatetic), contractors' employees working long term at the school and school governors and volunteers
- All aspects of the School's facilities where they are used by visitors, voluntary, statutory or community organisations.

2.2 The City of London School for Girls will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- A list of authorised persons who have various responsibilities for eSafety
- A range of policies including acceptable use policies that are frequently reviewed and updated
- Information to parents that highlights safe practice for children and young people when using the internet and other digital technologies;
- Adequate training for staff and volunteers
- Adequate supervision of pupils when using the internet and digital technologies
- Education that is aimed at ensuring safe and responsible use of internet and digital technologies
- A reporting procedure for abuse and misuse
- The school reserves the right to monitor the pupils' mobile and digital technologies and online activity through search engines and social media.

3. Roles and responsibilities

3.1. Technical Staff

Technical staff, led by the Director of IT and the Systems Manager, 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. They are responsible for maintaining appropriate filtering of the internet and 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 by girls to the Deputy Head (pastoral) who is also the DSL, and to the E-safety Coordinator.

3.2. E-safety Coordinator

The E-safety Coordinator is responsible for devising and implementing a coherent approach to e-safety across the school as part of safeguarding, in consultation with the Director of IT, the DSL and the Head of PSHCEE, and in line with national best practice recommendations.

He/She is responsible for staff training on e-safety, for ensuring that there is an age appropriate e-safety curriculum for pupils on the responsible and safe use of IT and for disseminating information to parents on all matters of e-safety. He/she is also responsible for monitoring , logging and reporting any breaches of the IT code of conduct by pupils using the internal monitoring system IMPERO. He/she is also responsible for the annual review and update of e-safety policies and procedures and for keeping an up-to-date log of any safety breaches to the IT and E-safety policy and actions taken.

3.3. Pastoral Staff

The DSL has ultimate responsibility for all matters of safeguarding of pupils, including e-safety.

The DSL will decide on appropriate sanctions in conjunction with relevant pastoral staff (tutors and heads of section) when breaches of the IT and e-safety policy occur in accordance with this policy, the school's Anti-bullying policy and the Sanctions and Rewards policy. The DSL is responsible for keeping a log of all bullying incidents (including cyberbullying) and actions taken.

The DSL will also refer more serious instances where the well-being and safety of a child is seriously compromised by their online activity to the LSCB, the Police, CEOPS, the Local Prevent Coordinator and local Channel panel as appropriate.

3.4 Staff

As stated in our Safeguarding and Child protection policy, it is ultimately the responsibility of all staff, teaching and support, contractors' employees working regularly on the premises and volunteers to ensure the safety of the pupils at the school. They should therefore all exercise vigilance in ensuring that pupils are using IT safely and responsibly and report all concerns to the e-safety Coordinator and the DSL.

4. Policies and procedures

We at The City of London School for Girls understand that effective policies and procedures are the backbone to developing a whole-school approach to eSafety. The policies that exist at the school are aimed at providing a balance between exploring the educational potential of new technologies and building the resilience and providing safeguards to pupils to protect themselves and their peers.

4.1 Use of Internet Facilities, Mobile and Digital Technologies

4.1.1 The City of London School for Girls will seek to ensure that internet, mobile and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

4.1.2 The City of London School for Girls expects all staff and pupils to use the internet, mobile and digital technologies responsibly and strictly according to the conditions below and to the IT Pupils' Code of Conduct and to the Staff's Acceptable Use of IT Policy, within the school's premises and beyond.[1] These expectations are also applicable to any voluntary, statutory and community organisations that makes use of the school's IT facilities and digital technologies.

Users shall not:

- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

    - Indecent still and moving images and sound files
    - Promoting discrimination of any kind
    - Promoting racial or religious hatred
    - Promoting illegal acts
    - Promoting extremist view and beliefs and terrorism
    - Any other information which may be offensive to peers or colleagues.

4.1.3 The School recognises that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded so that it can be justified if required. Permission to access such sites supported by the relevant justification must be sought from the E-safety coordinator and the Director of IT. In some cases the Deputy Head Academic or Pastoral or the Headmistress will need to be contacted.

4.1.4 Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- The promotion and advocacy of Extremism, violence, bomb making and terrorism
- Illegal taking or promotion of drugs

[1] For the purposes of this document, Internet usage means any connection to the internet via web browsing, external email, news groups or messaging services, mobile technologies e.g. mobile phone, including Bluetooth applications, tablets etc. including 3G or 4G connection.

- Software piracy
- Other criminal activity

4.1.5 In addition, users may not:

- Use the City of London's or an equivalent broadband provider's facilities for running a private business.
- Enter into any personal transaction that involves City of London or member Local Authorities in any way.
- Visit sites that might be defamatory or incur liability on the part of the City of London or member Local Authorities or adversely impact on the image of the City of London.
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of the City of London, or to the City of London itself.
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
    - financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships.
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet.
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate.
- Transmit unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.
- Assist with unauthorised access to facilities or services accessible via the school's network.
- Undertake activities with any of the following characteristics:
    - wasting staff effort or networked resources, including time on end systems accessible via the school's network and the effort of staff involved in support of those systems;
    - corrupting or destroying other users' data;
    - violating the privacy of other users;
    - disrupting the work of other users;
    - using the City of London School for Girls' network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
    - continuing to use an item of networking software or hardware after the City of London School for Girls has requested that use cease because it is causing disruption to the correct functioning of the school's network;

- other misuse of the City of London School for Girls network, such as introduction of viruses.

- Use mobile technologies 3/4G or mobile internet services in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

4.2 Reporting Abuse and Misuse

If a pupil is in breach of the Information technology and e-safety policy, it should be reported to the E-safety Coordinator and the relevant pastoral staff (tutor, head of section and/or Deputy Head pastoral) using the online Cause for Concern system.

If a pupil is involved in or the subject of any type of online abusive or exploitative behavior via any form of electronic communication, including social media, it must be reported immediately to the DSL. Staff who have such concerns reported to them must pass it on to the DSL. Concerns may include bullying, harassment, grooming, child sexual exploitation, stalking or being drawn into terrorism.

In accordance with the Safeguarding and Child Protection Policy, staff may contact the LADO directly, or when there is evidence that the pupil is already engaged in illegal activity, including terrorism, the Police. Relevant contact details are in the Safeguarding and Child Protection Policy.

If a member of staff is in breach of the Information technology and e-safety policy, it should be reported to the Deputy Head (staff).

Staff may contact the police directly if there is evidence that the member of staff is already engaged in illegal activity including terrorism.

If a member of staff is involved in or the subject of online abuse via email of other form of electronic communication such as social media by another member of staff, it should be reported to the Deputy Head (staff).

If a pupil or a member of staff accidentally accesses a website that contains abusive material they should immediately report this to the E-safety Coordinator.

Parents should bring any e-safety concerns to the attention of the e-safety coordinator or the DSL.

5 Education and training

5.1 The City of London School for Girls recognises that the internet and other digital technologies can transform learning, help to improve outcomes for children and young people and promote creativity; all of which add up to a more exciting and challenging classroom experience.

5.2 As part of achieving this, we want to create within City of London School for Girls an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils to have the skills and knowledge to enable them to use the internet and other digital technologies safely.

5.3 To this end, The City of London School for Girls will:-

- Provide a comprehensive programme of e-safety education to enable all pupils to stay safe online by becoming aware of the main threats posed to their safety and personal identity online, how to build resilience and how to report concerns. Pupils will be taught how to use technology responsibly, including what constitutes illegal use of online technologies and how to take care of their digital footprint, and how to exercise the skills of critical awareness, digital literacy and good online citizenship as part of PSHCEE and Computer Science. They will also be taught to understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy; recognise inappropriate content, contact and conduct and know how to report concerns.

- Educate school staff so that they are equipped to support pupils in gaining positive experiences when online and can help pupils develop strategies if they encounter a problem. Training on e-safety matters is carried out annually as part of the school's annual safeguarding training.

- Support parents in gaining an understanding of the policies and procedures that govern the use of internet and other digital technologies for all pupils at all times as well as providing them with up-to-date advice on how to best support their children's responsible and safe use of technologies at home. Parents can access an e-safety page on the portal with relevant resources and parent information evenings are organised regularly to disseminate information.

.

- Foster pupil resilience to extremism through the active promotion of British values and due regard to the Prevent Duty.

- Provide appropriate filtering of internet access through school or wireless system.

6 Infrastructure and technology

6.1 Partnership working

The City of London School for Girls will, as part of its wider safeguarding responsibilities, seek to ensure that voluntary, statutory and community organisations take an approach to their activities that sees the welfare of the child as paramount. To this end, we expect any organisation using the school's IT or digital

technologies to have appropriate policies and procedures that are aimed at safeguarding children and young people and reporting concerns. Relevant checks will be carried out by the Bursar.

7 Standards and inspection

The City of London School for Girls recognises the need to have regular reviews of policies and procedures in order to ensure that its practices are effective and that the risks to pupils are minimised. The Safeguarding and Child Protection policy is reviewed annually, and so are the Information Technology and E-safety Policy, the Pupil's IT Code of Conduct and the Acceptable User policy for staff. A report on e-safety matters is part of the annual safeguarding report that goes to the Board of Governors.

7.1 Monitoring

7.1.1 Monitoring the safe use of the internet and other digital technologies goes beyond the personal use of the internet and electronic mail that any pupil or member of staff may have. City of London School for Girls recognises that in order to develop an effective whole school eSafety approach there is a need to monitor patterns and trends of use inside school and outside school (Education and Inspections Act 2006, Section 89(5)).

7.1.2 With regard to monitoring trends within the school and individual use by school staff and pupils, City of London School for Girls will audit the use of the internet and electronic mail in order to ensure compliance with this policy. The school will also work with its internet service provider to further ensure compliance.

7.1.3 The E-safety Co-ordinator keeps a log of all breaches to the IT and E-safety policy and actions taken.

7.1.4 Filtering is applied to the school network and to the wireless network. Websites are blocked in categories and restrictions vary in age-appropriate ways. There is no access to any illegal material as detailed in 3.1. Staff or parents can also report additional websites that they believe should be blocked via the IT Support Help Desk by emailing itsupport@clsg.org.uk.

7.1.5 A Mobile Device Management (MDM) system is used to administer the deployment, security, monitoring and integration of school issued mobile devices within the school environment. Its intention is to optimise the functionality and the security of mobile devices by providing device configuration settings including device functionality, application and cloud restrictions.

7.1.6 In addition, monitoring of the students' use of the IT network is carried out using a system called IMPERO This system takes a

screenshot of any inappropriate language when using any software or a web browser. The screenshots record information about the user and can then be accessed via email.

7.2 Sanctions

7.2.1 The City of London School for Girls has been careful to develop policies and procedures to support the innocent in the event of a policy breach and enable the School to manage such situations in, and with, confidence.

7.2.2 Where there is inappropriate or illegal use of the internet and digital technologies, and therefore a breach of the Information technologies and E-safety (Policy 9 and its appendixes) has occurred, the following sanctions will be applied:

- Child / Young Person
    - The child/young person will be disciplined according to the Sanctions and Rewards policy, and/ or the Anti-bullying policy as appropriate. Sanctions may vary from a detention or withdrawal of access to the school network or internet, to suspension or exclusion in more extreme cases.
    - Serious breaches may lead to the incident being reported to the Police, CEOPS, the LADO, Children's Social Care, the Prevent Coordinator, the local Channel panel (as appropriate) or other regulatory bodies.
- Adult (Staff and Volunteers)
    - The adult may be subject to the City of London's disciplinary policy if it is deemed he/she has breached the Information Technology and eSafety Policy and its appendixes and/or the Employee Code of Conduct, the Corporation of London's Social Media Policy, the Safeguarding Policy and/ or the Teachers Standards.
    - Serious incidents that involve breaches to the Safeguarding and Child Protection Policy, the Prevent Duty and the Teachers' Standards may also lead to the incident being reported to the Police, the NCLT, the DBS, the LADO, the Prevent Coordinator or the local Channel panel as appropriate.

8 Working in partnership with parents and guardians

8.1 The City of London School for Girls is committed to working in partnership with parents and guardians and understands the key role they play in the internet safety of their children, through promoting internet safety beyond the school premises. Parents are issued with a copy of this policy and its appendixes upon their daughter entering the school and will receive all relevant updates.

8.2 The E-safety coordinator is responsible for the regular dissemination of up-to-date information to parents and for the organisation of parental information evenings to enable parents to support their children's safe and responsible use of technologies.

8.3 The City of London School for Girls also appreciate that there may be some parents who are concerned about the use of the internet, email and other digital technologies in school. In such circumstances school staff will meet with parents and guardians to discuss their concerns and agree how to allow their child to fully access the curriculum, whilst remaining safe.

This policy must be read in conjunction with:

- Safeguarding and Child Protection Policy and its Annexes
- Sanctions and Rewards Policy
- Anti-Bullying Policy
- Pupil Code of Conduct
- Behaviour Management Policy
- Pastoral Care, Discipline and Exclusions Policy
- Teachers' Standards
- Data Protection Policy
- City of London Corporation Data Protection Policy.
- City of London Corporation Employee Code of Conduct
- City of London Corporation Disciplinary Policy
- City of London Corporation Social Media policy

9 APPENDICES OF THE E-SAFETY POLICY

9.1 PUPILS' IT CODE OF CONDUCT

The IT Code of Conduct applies to all pupil users of Information Technology (IT) at City of London School for Girls while on the school premises or beyond.

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, 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, still or moving images, sound files 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.

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.
- During lessons, 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 computer settings 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.
- 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.

9.2 Staff Acceptable Use of IT Policy

9.2.1 Introduction

This policy is concerned with the security and authorised use of Information Systems (IS), including mobile telephones and iPADs provided to assist employees in the performance of their work duties. It is based on the City of London's 'IS and Communication Use' policy.

This policy will not breach an individual's right to privacy.

9.2.2 General Principles

Individuals are responsible for ensuring their unique user credentials for all work related information systems, including network access, are kept confidential (i.e. not shared with colleagues or written down and left in a non-secure place) and protected from misuse. Individuals are additionally responsible for "locking" their computer equipment whenever it is left unattended to ensure that unauthorised access is prevented.

9.2.3 Individuals should never:

- Use a colleague's user credentials to gain system access;
- Deliberately introduce viruses or other malware into a system;
- Disable antivirus software or inactivity timeouts set on their computer;
- Attempt to bypass or subvert system security controls, or use them for purposes other than those intended.

9.2.4 All communications equipment and information systems provided by the organisation remain the City of London School for Girls' property at all times and must not be removed from the business premises without the prior approval of the IT Department.

9.2.5 Whilst equipment and systems are provided for organisational use, limited and reasonable personal use will be permitted provided it does not negatively impact on service delivery.

9.2.6 Software must be used within the scope of the copyright and the terms and conditions of the end user licence agreement and any other applicable licences governing its use.

9.2.7 Employees must minimise the possibility of introducing malicious software to the City of London School for Girls' information systems e.g. by not opening unreliable or unknown data sources via e-mail or the internet.

9.2.8 City of London School for Girls data must be stored on the school's infrastructure only, except in limited circumstances where the temporary storage of data on non-City of London School for Girls equipment is permitted. All City data must be held in accordance with Data Protection principles. Work carried out on equipment without access to the network must be backed up regularly, uploaded to the network at the earliest opportunity and deleted from local drives.

9.2.9 Data must only be copied to removable or mobile media (e.g. laptop, VD, CD, mobile phone, etc) after an assessment of the risk of the device being lost, stolen or compromised has been made (i.e. consideration should be given to the sensitivity of the data). City data, regardless of its sensitivity, which is held on all such devices, should wherever practical be encrypted using the approved City encryption software or hardware device.

9.2.10 Limited (less than 10mb) non-work related data may be stored on the City of London School for Girls' IT infrastructure at the individual's own risk. Under no circumstances, however, should it be used to store unauthorised software or illegal copies of data such as music, films or images.

9.2.11 Access to certain data sources will be limited (e.g. inappropriate internet sites) in line with our commitment to equality and diversity or to safeguard our IT infrastructure.

9.2.12 Inappropriate (as defined by the Computer Misuse Act 1990, as covered in this policy) or excessive IT use is likely to constitute misconduct and be subject to the City of London's Disciplinary Procedure or criminal proceedings. The following are specifically prohibited:

- Attempting to access information or systems to which you have no right or authority;
- Connecting unauthorised or unlicensed devices or software to the school's infrastructure;
- Receiving or disseminating inappropriate or offensive material.

9.2.13 Further advice on this policy can be sought from the school's HR representative.

9.3 RESPONSIBILITIES

9.3.1. The IT Departmental staff are responsible for the security of the school's infrastructure and the maintenance of IT equipment.

9.3.2. Employees are responsible for the security of the IT equipment they operate and access to systems via their unique user credentials. Employees should, therefore, make themselves familiar with any security

policies, procedures or special instructions which relate to the information systems they use.

9.3.3. Employees must report any issues that breach this policy, or the related appendices, (including receipt of offensive materials via e-mail) to their line manager immediately.

9.4 MONITORING

9.4.1 IT use is routinely monitored corporately via the analysis of e-mail traffic, internet sites accessed and telephone records of calls made and received. Information on issues within City of London departments are provided to the Chief Officer to manage, in line with the City of London's employee data protection policy and code of conduct both of which can be found on the City of London's intranet.

9.4.2 The content of communication is not routinely monitored across the City of London, however, in specified circumstances such monitoring may be considered appropriate e.g. telephone calls being monitored for training purposes; where serious misuse of IT is suspected; or where potential criminal activity is suspected.

9.4.3. The reasons for, and conditions of, covert monitoring of the use of IT systems by individuals will be set out, in writing, in advance of such monitoring taking place.

Covert monitoring will only occur in circumstances where:

- Legislative provision allows for it; or
- Informing the individual would prejudice a criminal investigation or be prejudicial to the interests of the City of London.

Advice must be sought from City of London's Director of HR prior to covert monitoring taking place.

9.5 STAFF INTERNET ACCESS STATEMENT

9.5.1 Introduction

This statement supports the Acceptable Use of IT Policy and sets standards on appropriate internet use.

This statement applies to those who use the City of London School for Girls' Information Technology (IT) core infrastructure to connect to the internet.

9.5.2 General Principles

Internet access is provided to employees at the City of London School for Girls to facilitate efficient working practices.

The City of London School for Girls allows limited personal internet access, i.e. during breaks or before/after shifts.

The internet must not be used:

- To create/maintain, store or transfer corporate data other than for agreed operational purposes
- To solicit or carry out business activities for personal gain
- For gambling or playing games
- To access, create/maintain, store, transfer or publish statements, images, information or sounds:

    - which are potentially offensive, abusive or defamatory especially in relation to equal opportunities and employee complaints or which could lead to co-workers invoking the City of London's employee complaints procedure.
    - which constitute as pornography, paedophilia or other inappropriate sexually related material.
    - which constitute illegal activity.
    - which would bring The City of London School for Girls' into disrepute if details became public.

    This is not an exhaustive list.

Inappropriate or excessive internet use may lead to action being taken either through the City of London's disciplinary procedure or as a criminal offence.

Internet access may be withdrawn if it is abused.

Access to websites may be restricted due to operational needs, to ensure system security or because of their inappropriate nature.

Requests to access blocked websites for genuine organisational reasons must be submitted to the IT Service Desk.

The IT department will only provide internet access support for business related purposes.

Any personal purchases or transactions (in accordance with paragraph 4 above) are made at the individual's own risk.

9.5.3 Responsibilities

Line managers will ensure that internet usage does not negatively impact upon operations within The City of London School for Girls.

9.5.4 Monitoring

Internet usage will be monitored corporately, with issues being reported to departmental Chief Officers to manage, in line with the City of London's Data Protection Policy and Code of Conduct.

9.6 STAFF EMAIL, MESSAGING & SOCIAL MEDIA USE STATEMENT

9.6.1 Introduction

This statement supports the Acceptable Use of IT Policy setting standards on appropriate use of the school's Messaging services. Messaging services are those which include, but are not limited to; Email, Instant Messaging (IM) and SMS Text Messaging (SMS) and for the purposes of this statement include access to and use of 3rd party Social Media sites (such as Facebook, Twitter).

City of London School for Girls Messaging services and Social Media access are provided in order to facilitate efficient working, and to use communications to pursue the aims and objectives of the school.

Except where specifically known otherwise, messaging services and Social Media should be considered an insecure method of communication. Before transmitting any City of London School for Girls data via messaging services due regard must be given to the sensitivity of the data and the impact of it being intercepted, mis-delivered or it being later forwarded by a third party. Published City of London advice should be followed. i.e. Advice on Data Security, Advice – Risk Analysis for Sensitive Data. These documents are available on the City of London's Intranet.

Emails, in common with all information stored in hard copy or electronic formats, may be subject to disclosure to third parties, including the subject of a particular email, under the Data Protection and/or Freedom of Information Act, and in court proceedings.

This statement applies to all those who use the City of London School for Girls Information Technology (IT) core infrastructure to access the City of London School for Girls email and messaging systems and 3rd party Social Media sites.

9.6.2 General Principles

The school provides a number of messaging and communications services. Employees should be aware of them and the differences between them so as to ensure they use the most appropriate communications channel.

Employees should be cognisant of the issues which may arise from the use of instant messaging or social media for any communication or as part of a transaction where the City of London faces a potential legal, financial or reputational risk. It is extremely important if legal action is to be taken by the City, or is threatened against the City, that all correspondence and documentation is preserved, and to be able to compile a full record of all communications. Any messaging or social media communications used in business transactions must be stored as part of the audit trail of a transaction.

Messaging systems and Social Media sites must not be used to send or receive statements, images, information or sounds which:

- could bring the City of London Corporation into disrepute;
- are potentially offensive, abusive or defamatory especially in accordance with the City of London's equal opportunities and employee complaints policies;
- solicit or carry out business activities for personal gain;

- display or disseminate pornography, paedophilia or other inappropriate sexually related material;
- divulge non-public City data to unauthorised third parties;
- would constitute illegal activity

The City of London School for Girls allows limited personal use of Corporate messaging services. This includes the sending of non-work related messages between work colleagues.

Inappropriate or excessive use may lead to action being taken either through the City of London's disciplinary procedure or as a criminal offence.

Consideration must be given to limiting messaging distribution lists to those recipients who need the information. Messages should never be sent to 'everyone' in the City of London without approval from the Headmistress.

Recipient lines of messages should be carefully checked prior to sending, so as to ensure that communications are not accidentally distributed inappropriately. When sending emails to groups of parents BCC must be used. If you are not sure how to do this seek advice from the IT department.

Consideration must be given to the general housekeeping of Inboxes, in line with the City of London's Records Management principles.

Wherever practical employees should use 'short-cuts' to documents held in shared drives or folders instead of attaching files.

Employees should minimise the possibility of introducing malicious software to the City of London School for Girls' IT Network (e.g. unsolicited or non-work related attachments should not be opened).

Access to some attached file types may be restricted based upon operational needs or to ensure system security.

All messages must be responded to in line with the City of London's Service Response Standards.

Messaging access may be withdrawn if it is abused.

If information as set out in paragraph 9 above is received, it must be reported via line management immediately.

Appropriate training is available via the City of London's Desktop Training Services.

9.6.3 Email

Email provides a written means of communication both internally and with 3rd parties. Communications can be initiated without the need for the recipient to be available as they can read and respond at a later time.

Usually a copy of emails sent and received are automatically kept. Emails should be retained only for as long as is necessary and in accordance with all applicable legislation governing the retention of written records.

All external emails will automatically include the following disclaimer notice:

THIS E-MAIL AND ANY ATTACHED FILES ARE CONFIDENTIAL AND MAY BE LEGALLY PRIVILEGED. If you are not the addressee, any disclosure, reproduction, copying, distribution or other dissemination or use of this communication is strictly prohibited. If you have received this transmission in error please notify the sender immediately and then delete this e-mail. Opinions, advice or facts included in this message are given without any warranties or intention to enter into a contractual relationship with the City of London unless specifically indicated otherwise by agreement, letter or facsimile signed by a City of London authorised signatory. Any part of this e-mail which is purely personal in nature is not authorised by the City of London. All e-mail through the City of London's gateway is potentially the subject of monitoring. All liability for errors and viruses is excluded. Please note that in so far as the City of London falls within the scope of the Freedom of Information Act 2000 or the Environmental Information Regulations 2004, it may need to disclose this e-mail. Website: http://www.cityoflondon.gov.uk

Employees should use the 'out of office assistant' to advise when they are unavailable to respond to an email and when they are due to return. All out of office messages should usually include the following:

Please note that there is no auto-forwarding from this mailbox. Urgent matters should be redirected to:- xxx email address and/or xxx contact number.

All emails should include your email signature in the corporate format.

9.6.4 Messaging

Messaging provides an instantaneous means of communication. The City of London supports the use of Messaging for work related activities for short and immediate communication where there is no legal, financial or reputational risk to the City.

Messaging should not be used for communicating financial, contractual or sensitive information, decisions, historic or other information that we must retain for statutory purposes.

Messaging conversations if kept, are subject to the Freedom of Information Act, Data Protection Act and Environmental Information Regulations, if the information is held at the time of the request being received by the City of London Corporation. They are also disclosable in legal proceedings.

9.6.5 Short Message Service (SMS) Text Messaging

SMS refers to text messages using a school phone on a City of London contract.

SMS provides a written means of communication both internally and with 3rd parties. Communications can be initiated without the need for the recipient to be available as they can read and respond at a later time.

SMS should not be used for communicating financial, contractual or sensitive information, decisions, historic or other information that we must retain for statutory or Council purposes where this information is not also recorded elsewhere.

SMS campaigns, contacting multiple members of the public, should only be undertaken with the approval of the Headmistress.

All SMS communications will usually be automatically retained. Employees should routinely delete these messages unless there is a specific business case for retaining them. Employees should be aware that although the City policy is not to record or keep SMS messages, other organisations and individuals with whom you communicate may have a different policy.

SMS records, are subject to the Freedom of Information Act, Data Protection Act and Environmental Information Regulations, if the information is held at the time of the request being received by the City of London Corporation. They are also disclosable in legal proceedings.

9.6.6 Social Media

All City of London Corporation employees must abide by the Social Media policy

Social Media is a term covering multiple forms of communications (blogging, tweeting, etc) through social media websites. Typically, this is a written means of communication with 3rd parties.

The nature of social media means that all communications should be regarded as public information which virtually any individual could see.

Employees are individually responsible for any content they publish on social media sites.

To be effective users of social media sites should be mindful of their audience:

- write in an appropriate style
- be conscious that English may not be their first language.
- be aware of what is being asked, and the answer you give.
- where appropriate, re-direct customers to other information sources such as the City of London School for Girls website, Public Relations, Contact Centre, etc.

Always exercise good judgement in communications and do not:

- disclose any non-public information
- make judgement upon, slur, demean or communicate in a derogatory manner.

- violate the City of London's privacy, confidentiality and legal guidelines. Please seek guidance and permission before publishing or reporting on conversations that are meant to be private or internal to the City of London.

Comply with copyright and where appropriate credit others for their work.

Participation in social media on behalf of the City is not a right but an opportunity. Please treat it seriously and with respect.

Social Media sites will each have their own data retention policy. In some cases this may extend to "never" deleting data.

Please refer to the school's Safeguarding and Child Protection Policy. The following section is taken from Annex B of the Child Protection Policy:

- Be extremely careful over the use of Facebook, YouTube and any other social media.
- Make sure your privacy settings on social networking sites are at the highest possible level to avoid IT savvy pupils being able to access any private material.
- Never accept a student, parent or a recent leaver as a "friend" on Facebook etc.
- If you need students, parents or recent former pupils to contact you via Facebook, Twitter or the like for a school related activity (e.g. for a team or trip), set up a special separate site and let the DSL and Director of IT know what you have arranged and why.
- Always use your school e mail address and students' school e mail addresses when communicating with pupils by email.
- For anything apart from the most routine delivery and return of work or any learning-related queries, copy in your HOD or another appropriate colleague to all e mail exchanges with students and parents.
- Use a school mobile phone rather than your private phone for school activities and contacting students and parents. If enough warning is given these can be borrowed from the school.
- Only contact a student on her mobile phone or keep her number on record if there is a real need to do so and make sure that you inform your HOD or another appropriate colleague about why you are doing so.
- Apply common sense and professional judgement in all your electronic contacts with students and parents.

Further advice and guidance on the use of social media and 'how to engage' is available on the City of London's Public Relations' web pages and employees should read this prior to engaging in public forums.

9.6.7 Monitoring

Line managers will ensure that messaging use does not negatively impact upon operations within the City of London.

Messaging usage will be monitored corporately, with issues being provided to departmental Chief Officers to manage, in line with the City of London's employee data protection policy and the code of conduct.