Carshalton High School for Girls

e-Safety Policy

Introduction

Carshalton High School for Girls (CHSG) promotes a culture in which the school is a safe place to learn. As part of the overarching Safeguarding policy the e-Safety Policy provides a detailed account of e-Safety issues. It is revised annually and should be read in conjunction with the excellent material from the Borough and CEOP.

The school's e-Safety policy is in place in order to enable CHSG its own decisions on balancing educational benefit with potential risk. The school's e-Safety Policy covers the safe use of the internet and electronic communications technologies such as mobile phones and wireless connectivity. The policy will highlight the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It will also provide safeguards and rules to guide staff, governors, students and visitors in their online experiences.

The school's e-Safety policy operates in conjunction with others including policies for Good Behaviour, Anti Bullying, Curriculum, Data Protection, Communication, Safeguarding plus any Home-School Agreement.

This e-Safety policy has been approved by the Sutton Local Safeguarding Children's Board.

1. Effective Practice in e-Safety

1.1 e-Safety depends on effective practice in each of the following areas:

- education for responsible ICT use by staff and students
- a comprehensive, agreed and implemented e-Safety policy
- secure, filtered communications are provided
- a school network that complies with the National Education Network's standards and specifications

2. e-Safety Audit

2.1 In order to assess the quality of the school's procedures the school will undertake a regular e-Safety audit. Appendix A outlines suitable questions that comprise a comprehensive audit of procedures.

3. Writing and Reviewing the e-Safety Policy

3.1 The school has appointed an e-Safety Co-ordinator. This is not a technical role. The Co-ordinator is responsible for leading policy and practice in relation to e-Safety.

3.2 Our e-Safety Policy has been written by the school, building on the London Borough of Sutton's e-Safety Policy and Government guidance. It has been agreed by senior management and approved by governors.

4. Learning and Teaching

4.1 Why the Internet and digital communications are important?

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and students.

4.2 Guidelines for Use

- The school's Internet access will be designed expressly for student use and will include filtering appropriate to the age of students
- Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and students
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- The school will ensure that the use of Internet derived materials by staff and students complies with copyright law
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

5. Managing Internet Access

5.1 Information system security

- School ICT systems security will be reviewed regularly
- Virus protection will be updated regularly
- Security strategies will be discussed with the Local Authority
- Regular back-ups performed

5.2 e-mail

- Students may only use approved email accounts on the school system
- Students must immediately tell a teacher if they receive an offensive email
- In email communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission
- Incoming email should be treated as suspicious and attachments not opened unless the author is known
- The school should consider how emails from students to external bodies is presented and controlled
- The forwarding of chain letters is not permitted
- Any email violation will be treated in accordance with our Good Behaviour Policy, including abusive language
- Email etiquette should be considered at all times and these are highlighted in the Communications Policy

5.3 Published content and the school website

- E-mail will be used as an acceptable means of communication and staff school e-mail addresses will be published on the website
- The Headteacher and the members of the Senior Leadership Team responsible for the website will take overall editorial responsibility and ensure that content is accurate and appropriate

5.4 Publishing students' images, video and work

- Photographs that include students will be selected carefully so that individual students cannot be identified or their image misused
- Consideration should be given to using group photographs rather than full-face photos of individual children
- Students' full names must not be used anywhere on a school website or other on-line space, particularly in association with photographs
- On joining the school parents will be asked to sign to give their permission for photographs of their child to be used for publicity/marketing purposes (Appendix B)

- Student image file names will not refer to the student by their full name
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories
- No photographs in school uniform are allowed to be published by students

5.5 Social networking and personal publishing

- The school will control access to social networking sites and will educate students in their safe use
- Newsgroups will be blocked unless a specific use is approved
- Students will be advised never to give out personal details of any kind which may identify them, their friends or their location
- Students should not place personal photos on any social network space without considering how the photo could be used now or in the future
- Students should be advised on security and encouraged to use online nicknames and set passwords to deny access to unknown individuals and to block unwanted communications
- Students should only invite known friends and deny access to others
- Facebook, Twitter, Instagram, LinkedIn and YouTube accounts used by the school serve as a means of sharing information generally and by others i.e. individual departments

5.6 Managing filtering

- The school will work with the Local Authority (LA) and other bodies like CEOP to ensure systems to protect students are reviewed and improved
- If staff or students come across unsuitable on-line materials, the site must be reported to a teacher and in turn the e-Safety Co-ordinator and Safeguarding lead.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable

5.7 Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security
- Students must ask permission from the supervising teacher(s) before making or answering a videoconference call
- Videoconferencing and webcam use will be appropriately supervised for the students' age

5.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
- The senior leadership team should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications
- Mobile phones will not be used during lessons in accordance with the Good Behaviour Policy. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden and students found doing so will be set sanctions in line with the Good Behaviour Policy and the Mobile Phone Policy
- Publishing any such material on any public forum is not permitted
- The use by students of cameras in mobile phones will be kept under review. Students may be permitted occasional use if directly related to curriculum matters
- Games machines including the Sony Playstation, Microsoft XBOX and others have Internet access which may not include filtering
- Care is required in any use in school or other officially sanctioned location.
- **Staff will be issued with a school phone for trips/visits and for emergency use to contact parents/carers in an emergency**
- The appropriate use of Managed Learning Environments will be monitored at all times

5.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

5.10 *Cloud Service*

- The new Cloud service for the school frees up access to the school ICT resources from a fixed PC by allowing access from anywhere that has Internet access. The school will pilot this technology and the key resources that staff need to access from home, such as SIMS.net, Home folders and shared folders have already been prepared.

5.11 Passwords

- Password reset: Staff accounts will have to have their password changed every three months
- Home devices/PCs saving passwords: Staff must ensure that they never save their password on any device they use as they risk compromising their account and therefore access to the school network
- Complex passwords: Staff will have to use “complex” passwords for their school computer accounts in future. Complex passwords will have to be a minimum length of eight characters and will need to use numbers, upper and lowercase and characters

6. Policy Decisions

6.1 Authorising Internet access

- All staff must read and sign the Staff ICT Acceptable Use Policy before using any school ICT resource. (Appendix C)
- The school will maintain a current record of all staff and students who are granted access to school ICT systems
- Students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement. This is done by students signing the Home/School Agreement on entry to the school. (Appendix D)
- Any person not directly employed by the school will be asked to sign the ICT Acceptable Use Policy before being allowed to access the internet from the school site
- SLT and selected members of staff will have different filtering conditions
- Staff will be allowed access to selected sites once these have been approved by the e-Safety Co-ordinator

6.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network
- The school cannot accept liability for any material accessed, or any consequences of Internet access
- The school should audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate and effective

6.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the **Headteacher’s** Whistle Blowing policy

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and the school's overarching Safeguarding policy
- Students and parents will be informed of the complaints procedure **(see school's Complaints Policy)** depending on the severity of the incident
- Students and parents will be informed of consequences for students misusing the Internet

6.4 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-Safety
- The school will initiate Parents' Forums to discuss these issues

7. Communicating e-Safety

7.1 Introducing the e-safety policy to students

- e-Safety rules will be posted in all rooms where computers are used and discussed with students regularly
- Students will be informed that network and Internet use will be monitored and appropriately followed up
- A programme of training in e-Safety will be developed, possibly based on the materials from CEOP
- The school will undertake CEOP accreditation for one or more members of staff to deliver the CEOP Think U Know training programme to 11-16 year-olds
- Regular publicity about sites promoting e-Safety
- Students will also be informed through ICT lessons and assemblies
- Access to the e-Safety Policy via the school website

7.2 Staff and the e-Safety policy

- All staff will be given the school's e-Safety policy and its importance explained in conjunction with the overarching Safeguarding policy.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues
- Staff should understand that phone or online communications with students can occasionally lead to misunderstandings or even malicious accusations
- Staff must take care always to maintain a professional relationship

7.3 Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the school's e-Safety policy in newsletters, the school brochure and on the school website
- The school will maintain a list of e-Safety resources for parents/carers

Carshalton High School for Girls
CHSG
Community | Harmony | Success | Growth

Appendix A

e-Safety Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-Safety policy. Many staff could contribute to the audit including: Designated Child Protection Co-ordinator, Faculty Leader Learning Support, e-Safety Co-ordinator, Network Manager and Headteacher.

Does the school have an e-Safety policy that complies with guidance Y/N

Date of latest review (at least annual):

The school e-Safety policy was agreed by governors on:

The policy is available for parents and carers at:

The responsible member of the Senior Leadership Team is:

The responsible member of the Governing Body is:

The Designated Child Protection Co-ordinator is:

The e-Safety Co-ordinator is:

Has e-Safety training been provided for both students and staff? Y/N

Is there a clear procedure for a response to an incident of concern? Y/N

Have e-Safety materials from CEOP and Becta been obtained? Y/N

Do all staff sign a Code of Conduct for ICT on appointment? Y/N

Are all students aware of the school's e-Safety rules? Y/N

Are e-Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all students? Y/N

Do parents/carers sign and return an agreement that their child will comply with the school's e-Safety rules? Y/N

Are all staff, students, parents/carers and visitors aware that network and internet use is closely monitored and individual usage can be traced? Y/N

Is personal data collected, stored and used according to the principles of the Data Protection Act? Y/N

Is internet access provided by an approved educational internet service provider which complies with DfE requirements (e.g. SWAN)? Y/N

Has the school web filtering policy been designed to reflect educational objectives and approved by SLT? Y/N

Appendix B

Carshalton High School for Girls

CHSG

Community | Harmony | Success | Growth

PHOTO, IMAGE & VIDEO CONSENT FORM

Name:

Relationship with School:
(Daughter's Name)

Address:

Telephone No(s):

Email Address:

I give consent for my photograph or video image to be used for matters relating to school or the curriculum and on occasions used for purposes of promoting the positive image of the school. These include items such as school displays, the prospectus, press releases, newsletters, the school's internet presence including its website and other Sutton Education publications.

I understand that my daughter's full name will not be published with the images.

Signed: ___________________________________ Date: ___________________

Carshalton High School for Girls
CHSG
Community | Harmony | Success | Growth

Appendix C

Acceptable Internet Use Statement

For Staff and Senior Students

The computer system is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's ICT Access Policy has been drawn up to protect all parties - the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

- To comply with Data Protection obligations, access must only be made via your own authorised account and password, which must not be made available to any other person. It is forbidden for all users to allow another person to use a PC with their computer account.

- Computers, especially in classrooms, must never be left unattended while logged on and all users are expected to log off or lock their computers to protect against unauthorised access
- All computers and Whiteboards will be switched off at the end of the day
- All Internet use should be appropriate to staff professional activity or student's education
- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is forbidden
- The school operates a managed computer service and any new ICT hardware or software provision must be commissioned via the ICT Support department. It is forbidden to install or attempt to install any software on the school computers
- Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed
- Users are responsible for e-mail they send and for contacts made that may result in e-mail being received
- The same professional levels of language and content should be applied to e-mail as for letters or other media, particularly as e-mail is often forwarded
- Users are responsible for e-mail they send and for contacts made that may result in e-mail being received
- Never open email attachments from unknown sources. Always delete them
- Posting anonymous messages and forwarding chain letters is forbidden
- Legitimate private use is acceptable, providing school interests are not compromised and it is within legal boundaries
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- If the computer Anti-virus system warns of a virus on your computer or key stick stop using the computer immediately and students must inform a teacher. Staff must inform the ICT Support department
- Social networking sites and mobile phone technology such as Facebook, Twitter and BBM should only be used for personal use in a safe atmosphere. Friendships and communication between staff and students is not permitted
- No launching of pictures to do with school shall be placed on the internet without prior permission

Staff and students requesting ICT access should sign a copy of this Acceptable ICT Use Statement and return it to the ICT Manager for approval and issuing of computer accounts.

Full Name: ……………………………………………………. Form/Post: ………………………………..

Signed: ……………………………………………………….. Date: ……………………………………..

Access Granted: ……………………......................... Date: ……………………………………..

Appendix D

Carshalton High School for Girls

CHSG

Community | Harmony | Success | Growth

To ensure that students succeed at the school it is vital that parents, students and the school work together in very close partnership.

As a school we want to ensure that every member of the school community is happy and successful and that is best achieved where there is close working between parents, student and the school.

As a school we will provide a safe, calm, orderly environment that is built on high expectations, mutual respect and support.

We will ensure on an individual basis that the needs of every student are met and provide a stimulating, rich learning experience that includes a range of extra-curricular activities.

Finally, we will reward success and celebrate your daughter's success and share that with you.

Vivien Jones
Headteacher

As a student I agree to:

- come to school regularly and on time, properly equipped and in correct uniform
- do all my work to the best of my ability and hand homework in on time
- take responsibility for my own actions and respect the environment and the needs and privacy of others
- keep parents informed on all school matters and consult teachers about matters which may affect my work
- treat others as I would expect others to treat me
- follow school rules and instructions in connection with use of ICT and the internet

As a parent/guardian I agree to:

- see that my/our daughter goes to school regularly, on time, properly equipped and in correct uniform
- make the school aware of any concerns or problems that might affect my/our daughter's work or behaviour. Notify the school of any unavoidable absence as soon as possible that day
- support the school's policies and guidelines for behaviour. I understand that should my daughter bring offensive weapons or illegal substances into school it is likely to result in an exclusion from the school
- support my/our daughter in homework and other opportunities for home-learning in line with the Homework Policy
- attend Parents' Evenings and discussions about my/our daughter's progress
- support and take an interest in all aspects of my/ our daughter's school life

Student's signature	Parent's/Guardian's signature