Carshalton High School for Girls

Excellence: everywhere, every day.

Online Safety Policy

Reviewed and Agreed by Carshalton Local Governing Body: Jun 2021

Next Review: Jun 2022

Policy Notes may be subject to review and revision at any time by the Carshalton Local Governing Body notwithstanding that the next review date has not been reached.

Review dates are for guidance only and whilst the intention is always to arrange reviews within the stated time frame all Policy Notes will remain in force until this has taken place and been formally approved by the Carshalton Local Governing Body.

Contents

Online Safety Policy

1. Statement of Intent

Carshalton High School for Girls believes the use of ICT in schools brings significant benefits. Recognising risk and teaching online safety ensures students remain safe and learn important digital life skills.

This document will set out the schools key principles that all members of the school community are expected to understand and respect in their use of digital devices and online activities.

This document should be read in conjunction with

- GLT Child Protection and Safeguarding Policy
- GLT IT Policy & Appendices (which includes the acceptable users agreement)
- GLT Photograph and Media Policy
- GLT GDPR & Freedom of information Policy
- Remote Learning Handbook Including the remote learning Protocols
- CHSG Communications Policy
- CHSG Good Behaviour Policy
- CHSG Mobile Device Policy

2. Roles and Responsibilities

2.1 Headteacher

To take overall responsibility for e-safety provision.

- to ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements
- to be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant
- to be aware of procedures to be followed in the event of a serious e-safety incident
- to receive and respond to regular monitoring reports from the Designated Safeguarding Lead
- to ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures

2.2 Online Safety Lead

- to take day-to-day responsibility for online safety and have a leading role in establishing and reviewing the school online safety policy
- to promote an awareness of and commitment to e-safeguarding throughout the school community
- to ensure that appropriate online safety education is embedded across the curriculum
- to liaise with school IT technical staff
- to ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- to be proactive in monitoring use of the school's systems and detecting online safety concerns

- to ensure that online safety incidents are recorded according to safeguarding record-keeping procedures as appropriate
- to facilitate training and advice for all staff
- to be regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from online safety matters

2.3 Computer Science Curriculum Leader

- to oversee the delivery of the e-safety element of the Computer Science curriculum
- to liaise with the E-safety Co-ordinator on e-safety matters as appropriate

2.4 Network Manager / IT Technician

- to report online safety related issues that arise to the HOY or Designated Safeguarding Lead
- to manage systems which enable logging of network and software activity, and to provide access and tracking reports when investigating incidents or concerns
- to maintain appropriate web-filtering systems

2.5 Teachers

- to embed online safety issues in all aspects of the curriculum and other school activities as appropriate
- to supervise and guide students when engaged in learning activities involving online and communications technology

2.6 All staff

- to read, understand and help promote the school's online safety policies and guidance
- to read, understand and adhere to the school staff Acceptable Use Policy and Bring Your Own Device (BYOD) protocol. (see GLT IT Policies and Appendices)
- to read and put in practice guidance set out in the Remote Learning Protocols
- to be aware of online safety issues related to the use of mobile phones, cameras and hand-held devices, monitor their use and implement current school policies with regard to these devices
- to report any suspected misuse or problem to the HOY or Designated Safeguarding Lead
- to maintain an awareness of current online safety issues and guidance e.g. through CPD
- to model safe, responsible and professional behaviours in their own use of technology
- to ensure that any digital communications with students and Parents are conducted on a professional level and only through school-based systems, in accordance with the Staff Acceptable Use Policy and Communications Policy

2.7 Students

- to read, understand and adhere to the Student Acceptable Use Policy and remote learning protocols
- to understand the importance of reporting abuse, misuse or access to inappropriate materials
- to know what action to take if they or someone they know feels worried or vulnerable when using online technology

- to know and understand school policy on the use of mobile phones, digital cameras and handheld devices
- to know and understand school policy on the taking / use of images and on cyber-bullying
- to understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy may cover their actions out of school
- to take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home

2.8 Parents / Carers

- to support the school in promoting online safety
- to read, understand and endorse the Student Acceptable Use Policy
- to sign the copy of the student Acceptable Use Policy
- to support and promote the school Student Acceptable Use Policy
- to consult with the school if they have any concerns about their child's use of technology

2.9 Governor

- to ensure that the school follows all current online safety advice to keep the students and staff safe
- to approve the Online Safety Policy and review the effectiveness of the policy
- the Governor with responsibility for Safeguarding will also liaise with the DSL on matters regarding Online Safety
- to support the school in encouraging parents and the wider community to become engaged in online safety activities

2.10 Handling Complaints

- the school takes reasonable precautions to ensure online safety. However, due to the scale and range of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device
- the school cannot accept liability for material accessed, or any consequences of Internet access or use of communications technology.
- the relevant Head of Year acts as first point of contact for any complaint.
- any complaint about staff misuse will be referred to the Headteacher.
- complaints of cyber bullying are dealt with in accordance with the Good Behaviour Policy by the Head of Year
- complaints related to child protection are dealt with in accordance with the Child Protection and Safeguarding Policy by the Designated Safeguarding Lead

3 Online Safety in the ICT Curriculum

Online Safety is covered in ICT lessons at both Key Stage 3 and 4.

Across Key Stage 3, students will be taught 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.

At Key Stage 4, students will be taught about threats to programs and data from attack, damage or unauthorised access through the Internet and how to protect themselves. They learn about the different social engineering techniques people use to get access to personal information and what measures can be put in place to ensure their identity is kept safe.

4 PSHE and RSE 2020 Curriculum

The new Government RSHE framework identifies the following areas that must be addressed by the end of secondary school:

4.1 Online and media

- rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- about online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- what to do and where to get support to report material or manage issues online
- the impact of viewing harmful content
- that specifically sexually explicit material e.g. pornography presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- that sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- how information and data is generated, collected, shared and used online

4.2 Internet safety and harms

- the similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image), how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online
- how to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

At CHSG in PSHE are guided by the PSHE Association which has further refined the government frameworks and suggests that:

4.4.1 By the end of KS3:

a) the importance of, and strategies for, maintaining a balance between school, work, leisure, exercise, and online activities
b) the different types of intimacy online and their potential emotional and physical consequences (both positive and negative)
c) indicators of positive, healthy relationships and unhealthy relationships.
d) how to safely and responsibly form, maintain and manage positive relationships.
e) the qualities and behaviours students should expect and exhibit in a wide variety of positive relationships (including in school and wider society, family and friendships)
f) strategies to identify and reduce risk from people online that students do not already know; when and how to access help
g) how to seek, give, not give and withdraw consent (in all contexts)
h) about the unacceptability of prejudice-based language and behaviour, offline and online including sexism, homophobia, biphobia, transphobia, racism, ableism and faith-based prejudice
i) the need to promote inclusion and challenge discrimination, and how to do so safely,
j) to recognise peer influence and to develop strategies for managing it.
k) to recognise financial exploitation in different contexts e.g. drug and money mules, online scams
l) to establish personal values and clear boundaries around aspects of life that they want to remain private; strategies to safely manage personal information and images online, including on social media
m) to understand how the manner in which people present themselves online can have positive and negative impact on them
n) to respond appropriately when things go wrong online, including confidently accessing support, reporting to authorities and platforms
o) how to identify risk and manage personal safety in increasingly independent personal safety
p) the characteristics of abusive behaviours, such as grooming, sexual harassment, sexual and emotional abuse, violence and exploitation; to recognise warning signs, and how to report abusive behaviours or access support for themselves or others

4.4.2 By the end of KS4:

a) the benefits of having a balanced approach to spending time online
b) the opportunities and potential risks of establishing and conducting relationships online, and strategies to manage the risks
c) the legal and ethical responsibilities people have in relation to online aspects of relationships
d) to recognise unwanted attention (such as harassment and stalking), and ways to respond and how to seek help
e) about the impact of attitudes towards sexual assault and to challenge victim- blaming, including when abuse occurs online
f) the skills to assess their readiness for sex, including sexual activity online, as an individual and within a couple
g) the law relating to abuse in relationships, including coercive control and online harassment

h) to evaluate ways in which their behaviours may influence their peers, positively and negatively, and in situations involving weapons or gangs
i) the benefits and challenges of cultivating career opportunities online
j) strategies to manage their online presence and its impact on career opportunities
k) the skills to challenge or seek support for financial exploitation in different contexts including online
l) that there are positive and safe ways to create and share content online and the opportunities this offers
m) strategies for protecting and enhancing their personal and professional reputation online
n) how data may be used with the aim of influencing decisions, including targeted advertising and other forms of personalisation online; with strategies to manage this
o) ways to identify risk and manage personal safety in new social settings, workplaces, and environments.
p) strategies for identifying risky and emergency situations, ways to manage these and get appropriate help, including where there may be personal safety legal consequences (e.g. drugs and alcohol, violent crime and gangs)

5 Conduct and Incident Management

All users must conduct themselves in accordance with the requirements of the relevant Acceptable Use Agreement

All Staff Must:

- understand the importance of misuse of or access to inappropriate materials and to be aware of the consequences
- report abuse, misuse or access to inappropriate materials
- adopt good e-safety practice when using digital technologies out of school
- realise that the school's Online Safety Policy covers their actions out of school
- know and understand school guidance on the use of mobile phones, digital cameras and hand-held devices
- know and understand school policies on the taking photographs and the use of images, and on cyber-bullying

6 Incident Management

At Carshalton High School for Girls:

- there is strict monitoring and application of the Online Safety Policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes
- support is actively sought from other agencies as needed (e.g. the local authority CEOP, UK Safer Internet Centre helpline) in dealing with online safety issues

- monitoring, recording and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety within the school
- parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible
- We will contact the Police if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law.

7 The ICT Infrastructure

Carshalton High School for Girls:

- has the educational filtered secure broadband connectivity through Schools Broadband
- uses a NetSweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged
- has installed a monitoring system Visigo that alerts any safeguarding concerns to the DSL who will take any appropriate action necessary
- ensures network health through use of anti-virus software
- is vigilant in its supervision of students' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older students have more flexible access
- ensures all staff and students accept and agree to an Acceptable Use Policy and understands that they must report any concerns
- requires staff to preview websites before
- informs all users that Internet use is monitored
- informs staff and students that they must report any failure of the filtering systems directly to the IT Support Team
- makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through policy and CPD; provides advice and information on reporting offensive materials, abuse / bullying etc. available for students, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA

8 Network management (user access, backup)

Carshalton High School for Girls:

- uses individual, audited log-ins for all users
- has guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- has teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful
- ensures that storage of all data within the school will conform to the UK data protection requirements
- ensures the network is used safely

- ensures staff read the school's online safety Policy
- ensures staff access to the schools' management information system is controlled through the user's network account
- provides students with an individual network log-in username
- ensures all students have their own unique username and password which gives them access to the Internet and email account
- makes clear that no one should log on as another user and makes clear that students should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network
- has set-up the network with a shared work area for students and one for staff. Staff and students are shown how to save work and access work from these areas
- requires all users to always log off when they have finished working or are leaving the computer unattended
- where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves
- requests that teachers and students do not switch the computers off during the day unless they are unlikely to be used again that day
- makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so
- makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs
- maintains equipment to ensure Health and Safety is followed
- has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role; e.g. teachers access report writing module; SEN coordinator - SEN data
- ensures that access to the school's network resources from remote locations by staff is restricted just as if they were logged onto the network locally
- does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted, e.g. technical support or MIS Support, our Borough Attendance Service accessing attendance data on specific children, parents using a secure portal to access information on their child;
- provides students and staff with access to content and resources through the approved Learning Platform which staff and students access using their username and password
- makes clear responsibilities for the daily back up of MIS and other important files
- has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements
- uses the DfE secure s2s website for all CTF files sent to other schools
- follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network
- ensures our wireless network has been secured to industry standard Enterprise security level / appropriate standards suitable for educational use

- ensures all computer equipment is installed professionally and meets health and safety standards
- ensures projectors are maintained so that the quality of presentation remains high
- reviews the school ICT systems regularly with regard to health and safety and security

9 Email

Carshalton High School for Girls:

- provides staff with an email account for their professional use
- will contact the Police if one of our staff or students receives an email that we consider is particularly disturbing or illegal
- will ensure that email accounts are maintained and up-to-date, including the disabling of obsolete accounts
- reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the Police

9.1 Student email:

Students are introduced to the use of email as part of the Computer Science scheme of work Students are taught about the safety and 'etiquette' of using email both in school and at home.

Students are taught:

- not to give out their email address unless it is part of a school managed project or is given to someone they know and trust and is approved by their teacher or parent / carer
- that an email is a form of publishing where the message should be clear, short and concise
- that they must not reveal private details of themselves or others in email, such as address, telephone number, etc.
- to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe
- that they should think carefully before sending any attachments
- that they must immediately tell a teacher / responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature
- that they should not respond to malicious or threatening messages
- that they should not delete malicious of threatening emails, but keep them as evidence of bullying

9.2 Email Monitoring :

All use of the school email system, including provision for monitoring and accessing content, is documented in the staff IT Acceptable Use Policy.