THE CAMDEN SCHOOL FOR GIRLS

E-Safety Policy

Lead Staff members:	R Bradshaw & B Raspudic
Review Date:	November 2021
Link Governor	Manuela Grayson
Approved by:	C&S Jan 2019 – then Headteacher approval

Contents

Overview

This Policy has been created using the guidance supplied by Camden Local Authority in their model online safety policy for schools and colleges in Camden published in September 2018 and the London Grid for Learning (LGfL) Digisafe online safety policy template for schools published in August 2018.

The governing body and senior leadership team at Camden School for Girls operate a procedure in line with local and national guidelines. They work to the following policy documents:

School Policies

- Child Safeguarding and Protection Policy
- Behaviour Policy
- Staff behaviour policy (code of conduct)
- Anti-Bullying Policy
- E-Security Policy
- Special Educational Needs Policy
- Data Protection policy
- Acceptable Use Policies
- Data breach Policy

Other documents

- 'Keeping Children Safe in Education' 2018 Part 1 Annex A
- 'Keeping Children Safe in Education' 2018 Full Document Annex A-H
- 'Working together to safeguard children' (DfE 2018)
- Sexual violence and sexual harassment between children in schools and colleges (DfE 2018)
- Online safety in schools and colleges: Questions from the Governing Board
- UKCCIS framework Education for a Connected World
- Data protection: a toolkit for schools (August 2018)
- Sexting guidance from UKCCIS - Overview for all staff

At Camden School for Girls the aim is to provide an environment in which students can thrive and reach their full potential. To achieve this the welfare and safety of our students is paramount and the e-safety policy is an integral part of fulfilling this aim.

The core principles of the policy are:

- Camden School for Girls will operate under the statutory procedures of Duty of Care and all binding interventions covered by The Children Act 1989, Education Act 2002, The Children's Act 2004 and DfE Statutory Guidance Working Together to Safeguard Children issued March 2018.
- Keeping children safe in education March 2018

Glossary

LGfL	London Grid for Learning

DOP	Data Protection Officer
LSCB	Local Safeguarding Children Board
DfE	Department for Education
OSL	Online Safety Lead
DSL	Designated Safeguarding Lead
SIRO	Senior Information Risk Owner
GDPR	General Data Protection Regulations
SLT	Senior Leadership Team
KCSIE	Keeping Children Safe in Education document
UKCCIS	UK Council for Child Internet Safety
CPD	Continuing Professional Development
PHSE	Personal, social, health and economic education
RSE	Relationship and Sex Education

INTRODUCTION

Camden School for Girls commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school and that those from outside school will continue to impact on students when they come into school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Online-safety is a part of safeguarding and general e-Safety concerns must be handled in the same way as any other safeguarding concern and any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

The school will actively seek support from other agencies as needed. We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or students engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

Aims

This policy aims to:

- Set out expectations for all Camden School for Girls community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld on the school premises and beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online

- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

Scope

This policy applies to all members of the Camden School for Girls community (including staff, governors, volunteers, students, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time.

Roles and responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, students, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Headteacher

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance
- Liaise with the designated safeguarding lead on all e-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of students, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff who carry out internal technical e-safety procedures

- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory DfE requirements

Designated Safeguarding Lead / Online Safety Lead – Ms K Derrar/Ms J Man

Key responsibilities (remember the DSL can delegate certain online-safety duties, e.g. to the online-safety coordinator, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education 2018):

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective approach to online safety that empowers the school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with the local authority and work with other agencies in line with Working together to safeguard children"
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the Headteacher, SIRO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends
- Ensure that online safety education is embedded across the curriculum and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with SLT to discuss current issues (anonymised), review incident logs and network infrastructure
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Oversee and discuss 'appropriate filtering and monitoring' with governors (is it physical or technical?) and ensure staff are aware (Ofsted inspectors have asked classroom teachers about this). If you use LGfL filtering, view the appropriate filtering statement here
- Ensure the 2018 Department for Education guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff:
    - all staff must read KCSIE Part 1 and all those working with children (Annex A of KCSIE)

- it would also be advisable for all staff to be aware of Annex C (online safety) (KCSIE)
- cascade knowledge of risks and opportunities throughout the organisation
- cpd.lgfl.net has helpful CPD materials including PowerPoints, videos and more

Governing Body, led by Online Safety / Safeguarding Link Governor – Mr J Atmore

Key responsibilities (quotes are taken from Keeping Children Safe in Education 2018):

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCCIS) Online safety in schools and colleges: Questions from the Governing Board.
- "Ensure an appropriate senior member of staff, from the SLT, is appointed to the role of DSL with lead responsibility for safeguarding and child protection (including online safety) with the appropriate status and authority and time, funding, training, resources and support…"
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the SIRO, DSL and Headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in your school
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction and regularly updated information in line with advice from the LSCB. Online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach." There is further support for this at cpd.lgfl.net
- "Ensure appropriate filters and appropriate monitoring systems are in place but be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding".
- "Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Consider a whole school approach to online safety a clear policy on the use of mobile technology."

All staff

Key responsibilities:

- Undertake regular Safeguarding and e-Safety training
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections)

- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy and code of conduct
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for students)
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what students are doing and consider potential dangers and the age appropriateness of websites
- To carefully supervise and guide students when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Encourage students to follow their acceptable use policy, remind them about it and enforce school sanctions
- Notify the DSL/OSL of new trends and issues before they become a problem
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
- Receive regular updates from the DSL and have a healthy curiosity for online safety
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

Sanctions for staff

These will reflect the seriousness with which any breach of acceptable use policies by staff members will be viewed given their position of trust and the need to ensure acceptable standards of behaviour by adults who work with children.

Category A infringements

These are minor breaches of the school's acceptable use policy which amount to misconduct and will be dealt with internally by the head teacher.

- excessive use of internet for personal activities not connected to professional development
- use of personal data storage media (eg: removable memory sticks) without carrying out virus checks
- any behaviour on the world wide web and social media sites such as Twitter that compromises the staff member's professional standing in the school and community, for example inappropriate comments about the school, staff or students or inappropriate material published on social networking sites
- sharing or disclosing passwords to others or using other user's passwords
- breaching copyright or licence by installing unlicensed software.

Possible sanctions include referral to the head teacher who will issue a warning

Category B infringements

These infringements involve deliberate actions that undermine safety on the internet and activities that call into question the person's suitability to work with children. They represent gross misconduct that would require a strong response and possible referral to other agencies such as the police or Camden's LADO.

- serious misuse of or deliberate damage to any school computer hardware or software, for example deleting files, downloading unsuitable applications
- any deliberate attempt to breach data protection or computer security rules, for example hacking
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute
- inappropriate contact by members of staff with pupils by email or social media

Possible sanctions include:

- referral to the head teacher
- removal of equipment
- referral to Camden's online safety officer
- referral to Camden's LADO or the police
- suspension pending investigation
- disciplinary action in line with school policies.

Refer to the following policies for more information:

- Staff behaviour policy (code of conduct)
- Disciplinary Policy and Procedures.

PSHE lead

Key responsibilities from September 2019 for September 2020 (quotes taken from DfE press release on 19 July 2018 on new relationships and health education in schools):

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / RE / RSE curriculum, "complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds."
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE

Computing Curriculum Lead

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Subject / Department leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or department, and model positive attitudes and approaches to staff and students alike
- Consider how the UKCCIS framework Education for a Connected World can be applied in your context
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing

Head of ICT Support/Network Analyst

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Keep up to date with the school's e-safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the DSL / OSL / SIRO to ensure that school systems and networks reflect school policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and SLT
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Monitor the use of school technology and online platforms such as Google Apps for Education, and that any misuse/attempted misuse is identified and reported in line with school policy
- Work with the Headteacher to ensure the school website meets statutory DfE requirements

Senior Information Risk Owner (SIRO) – Ms R Bradshaw

Key responsibilities:

- Be aware of the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (April 2018), especially this quote from the latter document:
    - GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place. Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding
- The same document states that the retention schedule for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'
- Work with the DSL, Headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

LGfL TRUSTnet Nominated contacts – Headteacher and Head of ICT Support

Key responsibilities:

- To ensure all LGfL TRUSTnet services are managed on behalf of the school in line with school policies, following data handling procedures as relevant
- Work closely with the DSL and SIRO to ensure they understand who the nominated contacts are and what they can do / what data access they have, as well as the implications of all existing services and changes to settings that you might request – e.g. for YouTube restricted mode, internet filtering settings, firewall port changes, sharing settings for any cloud services such as Google G Suite.
- Ensure the SIRO is aware of the GDPR information on the relationship between the school and LGfL TRUSTnet at gdpr.lgfl.net

Volunteers and contractors

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology

Students

Key responsibilities:

- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Category A infringements

These are low-level breaches of acceptable use agreements such as:

- use of non-educational sites during lessons
- unauthorised use of email or mobile phones
- unauthorised use of prohibited sites for instant messaging or social networking.

Sanctions could include referral to the Form tutor or Head of Year, removal of mobile phone until the end of the day, as well as a referral to the online safety co-ordinator.

Category B infringements

These are persistent breaches of acceptable use agreements following warnings and use of banned sites or serious breaches of online safety policy that are non-deliberate, such as:

- continued use of non-educational or prohibited sites during lessons
- continued unauthorised use of email, mobile phones or social networking sites during lessons
- use of file sharing software
- accidentally corrupting or destroying other people's data without notifying staff
- accidentally accessing offensive material without notifying staff.

Sanctions could include:

- referral to form tutor or Head of Year
- referral to online safety co-ordinator
- loss of internet access for a period of time
- removal of mobile phone until the end of the day
- contacting parents.

Category C infringements

These are deliberate actions that either negatively affect school ICT systems or are serious breaches of acceptable use agreements or anti-bullying policies, such as:

- deliberately bypassing security or access
- deliberately corrupting or destroying other people's data or violating other's privacy
- online bullying
- deliberately accessing, sending or distributing offensive or pornographic material
- purchasing or ordering items over the internet
- transmission of commercial or advertising material.

Sanctions could include:

- referral to form tutor or Head of Year
- referral to online safety co-ordinator
- referral to head teacher
- loss of access to the internet for a period of time
- contact with parents
- any sanctions agreed under other school behaviour policy.

Category D infringements

These are continued serious breaches of acceptable use agreements following warnings or deliberately accessing and distributing banned or illegal materials which may result in a criminal offence, such as:

- persistent and/or extreme online bullying
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute.

Sanctions could include:

- referral to head teacher
- contact with parents
- possible exclusion
- removal of equipment
- referral to community police officer
- referral to Camden's online safety officer.

Students with special educational needs and disabilities (SEND) and SEND Co-ordinators

Students with learning difficulties or disability may be more vulnerable to risk from use of the internet and may need additional guidance on online safety practice as well as closer supervision.

SEND co-ordinators are responsible for providing extra support for these students and should:

- link with the online safety co-ordinator to discuss and agree whether the mainstream safeguarding systems on the internet are adequate for students with SEND
- where necessary, liaise with the online safety co-ordinator and the IT service to discuss any requirements for further safeguards to the school IT system or tailored resources and materials in order to meet the needs of students with SEND

- ensure that the school's online safety policy is adapted to suit the needs of students with SEND
- liaise with parents, carers and other relevant agencies in developing online safety practices for students with SEND
- keep up to date with any developments regarding emerging technologies and online safety and how these may impact on students with SEND.

Parents/carers (including members of parent associations)

Key responsibilities:

- Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, students or other parents/carers.

Visitors

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, students or other parents/carers

AREAS OF FOCUS IN E-SAFETY

Education and curriculum

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- PSHEE
- Health Education, Relationships and Sex Education (being implemented from September 2019 for September 2020)
- Computing
- Citizenship

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for students).

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what students/students are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide students when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

At Camden School for Girls we recognise that online safety and broader digital resilience must be threaded throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World' from UKCCIS (the UK Council for Child Internet Safety, soon to become UKCIS, no longer solely for children).

Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding as well as being a curriculum strand of Computing, PSHE, Citizenship and (from September 2019 for September 2020) the new statutory Health Education and Relationships and Sex Education.

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Non-teaching staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online-safety will be mostly detailed in the following policies

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Data Protection Policy

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school and that those from outside school will continue to impact on students when they come into school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline on 0344 381 4772, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or students engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting; see section below).

Sexting and sexual abuse and harassment by peers

The school will refer to the UK Council for Child Internet Safety (UKCCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The internet contains a high level of sexually explicit content and internet-based communications systems and social networking sites can be used to send sexually explicit messages and images. In some cases these actions may be harmful or abusive or may constitute harassment or online bullying. "Sexting" or the sending of sexual images between young people via the internet or mobile devices is a particular issue young people need to know that producing and sharing these images is illegal. Students need to understand that once the image is sent, they have lost control of who it is distributed to and how it is used, and that there is a good chance that the image will be widely seen, possibly including parents.

Staff need to be able to react to incidents in a proportional manner so that the welfare of young people is safeguarded and no young person is unnecessarily criminalised. Guidance for responding to incidents is available at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF

Staff need to be aware of the use of IT by older students for the purpose of distributing unsuitable materials and sexually harassing other students and be able to safeguard students from this.

The school DSL will in turn use the full 50-page guidance document including case studies, typologies and a flow chart as shown below (for information only, must be viewed in the context of the full document) to decide next steps and whether other agencies need to be involved. It is important that everyone understands that whilst sexting is illegal, students can come and talk to members of staff if they have made a mistake or had a problem in this area.

The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net

Bullying

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying.

Risk from inappropriate contacts with adults

Teachers may be concerned about a student being at risk as a consequence of their contact with an adult they have met over the internet. The student may report inappropriate contacts or teachers may suspect that the student is being groomed or has arranged to meet with someone they have met on-line. School staff should also be aware of students being sexually abused on-line through video messaging such as Skype. In these cases, perpetrators persuade the young person concerned to carry out sexual acts while the perpetrator watches/records.

- All concerns around inappropriate contacts should be reported to the online safety co-ordinator and the designated safeguarding lead.
- The designated safeguarding lead should discuss the matter with the referring teacher and where appropriate, speak to the student involved, before deciding whether or not to make a referral to Children's Safeguarding and Social Work and/or the police.
- The police should always be contacted if there is a concern that the child is at immediate risk, for example if they are arranging to meet the adult after school.
- The designated safeguarding lead can seek advice on possible courses of action from Camden's online safety officer in Children's Safeguarding and Social Work.
- Teachers will advise the student on how to terminate the contact and change contact details where necessary to ensure no further contact.
- The designated safeguarding lead and the online safety co-ordinator should always notify the student's parents of any concerns or incidents and where appropriate, arrange to meet with them discuss what action they can take to ensure their child's safety.
- Where inappropriate contacts have taken place using school IT equipment or networks, the online safety co-ordinator should make a note of all actions taken and contact the network manager or learning platform provider to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other students is minimised.

Risk from contact with violent extremists

Many extremist groups who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences and may be radicalised as a result.

Staff members have a duty under the Government's Prevent programme to prevent vulnerable young people from being radicalised and drawn into terrorism. The main mechanism for this is Camden's Channel

Panel, a multi-agency forum that identifies young people who are at risk and develops a support plan to stop the radicalisation process and divert them from extremism.

- Staff have received training regarding the school's duty under the Prevent programme and the need to recognise any student who is being targeted by violent extremists via the internet for the purposes of radicalisation. Students and staff will be warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies.
- The school will ensure that adequate filtering is in place and review filtering in response to any incident where a student or staff member accesses websites advocating violent extremism.
- All incidents will be dealt with as a breach of the acceptable use policies and the school's behaviour and staff disciplinary procedures will be used as appropriate.
- The online safety co-ordinator and the designated safeguarding lead will record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school and whether current school procedures are robust enough to deal with the issue.
- Where there are concerns that a young person is being radicalised or is in contact with violent extremists, or that their parents are and this is placing the child or young person at risk, schools will refer the young person to the Channel Co-ordinator for support.

Further information is available in the CSCB guidance "Safeguarding children and young people from radicalisation and extremism" available at: https://cscb-new.co.uk/?page_id=8128

Risk from sites advocating suicide, self-harm and anorexia

Some internet sites advocate dangerous activities such as self-harming, suicide or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse.

Exposure to potentially harmful materials online may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.

- The school will ensure that young people have an opportunity to openly discuss issues such as self-harming, suicide, substance misuse and anorexia as part of the PHSE curriculum.
- Pastoral support will be available to all young people to discuss issues affecting them and to establish whether their online activities are an added risk factor
- Staff will receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help.

Sexual violence and harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL. Staff should work to foster a zero-tolerance culture.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology such as school cameras.

Where students contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Camden School for Girls community. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the school behaviour policy (for students) or code of conduct (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Camden School for Girls will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Data protection and data security

All students, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements.

The Headteacher, SIRO and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions

- CCTV – Recordings are kept for a maximum of 7 days. Access to the recordings should be requested by the members of SLT
- Access to the CCTV recordings from third parties should be requested via Senior Information Risk Owner (SIRO) in writing using the appropriate request forms.

- A central record of user login and passwords are kept securely by the Head of ICT Support, if your password is compromised, this needs to be changed immediately by the IT support team
- All individuals using the school system should ensure that they log off when they have finished using a device and should never leave a device unlocked and unattended
- Backups – daily backup of internally stored data, weekly backups taken off site, tapes reused every 4 weeks
- Security processes and policies
- Disaster recovery
- Access by third parties, e.g. IT support agencies – only with assistance from the ICT department
- BYOD – students, staff and visitors can bring their own devices
- Wireless access – only available to staff, students, visitors and lettings using guest logins or those created for a specific purpose upon request but have no access to networked files/drives
- File sharing – restricted within the school domain
- Cloud platform use, access and sharing protocols - school recognises the benefits of cloud computing platforms, to enhance teaching and learning and makes use of Google Apps for Education. Sharing files is restricted to users within the school domain to avoid possible sharing of sensitive data outside the organisation.

Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place and not be able to access harmful or inappropriate material but at the same time be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

At this school, the internet connection is provided by LGfL TRUSTnet. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen, which is made specifically to protect children in schools. In addition to the LGFL filtering system we use internally configured solutions (DNS, firewall) to provide more flexibility for teachers and use of digital resources.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom)
2. Internet and web access
3. Active/Pro-active technology monitoring services

At Camden School for Girls we use a combination of options 1 and 2 above.

Electronic communications

Email

- Students and Staff at this school use Google Apps for Education which includes Gmail for all
- Google Apps for Education are the only means of electronic communication to be used between staff and students

- Parentmail, ParentPay and school Gmail accounts are the only forms of electronic communication to be used between staff and parents
- Use of a different platform must be approved in advance by the SIRO / Headteacher in advance. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member)
- Electronic communications may only be sent using the systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/ SIRO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- Students and staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination

See also the social media section of this policy.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher has delegated the day-to-day responsibility of updating the content of the website to the Head of ICT Support and delegated administration staff.

The site is managed by e4Education.

The Department for Education has determined information which must be available on a school website. LGfL TRUSTnet has compiled RAG (red-amber-green) audits to help schools to ensure that are requirements are met (see appendices).

Where other staff submit information for the website, they are asked to remember:

- School have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name)

Cloud platforms

Camden School for Girls recognises the benefits of cloud computing platforms, not just for cost savings but to enhance teaching and learning and makes use of Google Apps for Education.

This school adheres to the principles of the Department for Education document 'Cloud computing services: guidance for school leaders, school staff and governing bodies'.

For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush –never share it with anyone!"), expert administration and training can help to keep staff and students safe, and to avoid incidents. The following principles apply:

- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work

Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos and used by the school.

Whenever a photo or video is taken/made, the member of staff taking it will check consent has been given before using it for any purpose.

Any students shown in public facing materials are never identified with more than first name.

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of students, and where these are stored. At Camden School for Girls no member of staff will ever use their personal phone to capture photos or videos of students.

Photos are stored on Team Drive in Google Apps for Education in line with the retention schedule of the school Data Protection Policy or on the internal server (network share) with limited access.

Staff and parents are reminded about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Students are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children.

Students are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Social media - Camden School for Girls SM presence

Camden School for Girls works on the principle that if we don't manage our social media reputation someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online (Mumsnet is a favourite).

Accordingly, even though we do not have an official social media presence, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

Staff, students' and parents' SM presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and students will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, students and parents, also undermining staff morale and the reputation of the school (which is important for the students we serve).

Many social media platforms have a minimum age of 13, but the school regularly deals with issues arising on social media with students/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our students/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). It is encouraging that 73% of students (from the 40,000 who answered that LGfL DigiSafe pupil online

safety survey) trust their parents on online safety (although only half talk about it with them more than once a year at the moment).

Students are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher, and should be declared upon entry of the pupil or staff member to the school.

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that of the 131 Prohibition Orders issued to staff in 2017, 73 involved social media/technology (and 27 of the 66 orders by August 2018).

Device usage

Personal devices and bring your own device (BYOD) policy:

- All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone
- Volunteers, contractors, governors should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Headteacher should be sought (the Headteacher may choose to delegate this) and this should be done in the presence of a member staff
- Parents are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document. parentfilming.lgfl.net may provide further useful guidance

Network / internet access on school devices/personal devices:

- Students are allowed access to the school WIFI via personal devices for school related use within the framework of the acceptable use policy with their school user accounts

- All staff working at the school are allowed access to the school WIFI via personal devices for school related use within the framework of the acceptable use policy with their school user accounts. Child/staff data should never be downloaded onto a private phone or other electronic device such as a laptop
- Volunteers, contractors, governors can access the wireless network using guest logins or those created for a specific purpose upon request but have no access to networked files/drives, subject to the acceptable use policy
- Internet filtering restrictions apply to all users using the school WiFi
- Parents have no access to the school network or wireless internet on personal devices

Trips / events away from school

For school trips/events away from school, teachers will be issued a school duty phone and this number is to be used for any authorised or emergency communications with students/students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by SLT have a statutory power to search students/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Full details of the school's search procedures are available in the school Behaviour Policy.

Appendix

1. Acceptable Use Policies (AUPs) for:
    - Students
    - Staff, Volunteers Governors & Contractors
    - Parents

2. Annex G Flowchart for responding to incidents

Annex G

Flowchart for responding to incidents