THE CAMDEN SCHOOL FOR GIRLS

Online Safety Policy

Lead Staff members: Kathia Derrar & Yasemin Briant

Review Date: Summer 2026

Last updated: Summer 2025

Contents

Overview

Aims

This policy aims to:

- Help safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads and beyond.
- 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 beyond the confines of the school gates and school day, and regardless of device or platform, and that the same standards of behaviour apply online and offline.
- 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/pupils, 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, or who use technology in their school role.

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, pupils, 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.

All staff

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the school's main safeguarding policy, the code of conduct/handbook and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

They must report any concerns, no matter how small, to the designated safety lead as named in the AUP, maintaining an awareness of current online safety issues and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

Staff should also be aware of the DfE standards for filtering and monitoring and play their part in feeding back to the DSL about overblocking, gaps in provision or pupils bypassing protections. All staff are also responsible for the physical monitoring of pupils' online devices during any session/class they are working within.

Headteacher – Ms K Law

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 Partnership support and 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 pupils, 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 (DSL) – Ms K Derrar

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

- The DSL should "take lead responsibility for safeguarding and child protection (including

online safety and understanding the filtering and monitoring systems and processes in place)."

- 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 whole school 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."
- Ensure the school is complying with the DfE's standards on Filtering and Monitoring. Camden School for Girls uses LGfL filtering and Lightspeed filtering and monitoring.
- 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 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/trustees
- 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 discuss how filtering and monitoring work and have been functioning/helping.
- 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
- Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying)
- Facilitate training and advice for all staff:
    - all staff must read KCSIE Part 1 and all those working with children also Annex B
    - this must include filtering and monitoring and help them to understand their roles
    - cascade knowledge of risks and opportunities throughout the organisation

Governing Body, led by Online Safety / Safeguarding Link Governor – Ms M Grayson

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

- 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 D on Online Safety reflects practice in your school
- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction and that this is updated
- "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 with a clear policy on the use of mobile technology"

PSHE lead

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from latest trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE / RE / RSE curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives."
- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app
- 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 / aspect leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and pupils 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:

- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology
- 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 Y Briant

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the DP and cyber security policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in Data protection in schools, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."
- 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
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil

Pupils

Key responsibilities:

Read, understand, sign and adhere to the student/pupil acceptable use policy.

Parents/carers

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.

External groups including parent associations

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, pupils or other parents/carers

Education and curriculum

Despite the risks associated with being online, Camden School for Girls recognises the opportunities and benefits of children being online. Technology is a fundamental part of our adult lives and so developing the competencies to understand and use it, are critical to children's later positive outcomes. The choice to use technology in school will always be driven by pedagogy and inclusion.

The teaching of online safety, features in these particular areas of curriculum delivery:

- PSHE
- 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.

Whenever overseeing the use of technology (devices, the internet, generative AI tools, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential risks and the age appropriateness of tasks.

This includes supporting them with search skills, reporting and accessing help, critical thinking (e.g. disinformation, misinformation and fake news), access to 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.

Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding and so 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 speak 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.

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
- Acceptable Use Policies
- Data Protection Policy

This school commits to take all reasonable precautions to safeguard pupils online but recognises that incidents will occur both inside school and outside school and that those from outside school will continue to impact on pupils 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 designated safeguarding lead as soon as possible on the same day. The reporting member of staff will ensure that a record is made of the concern on CPOMS - this includes any concerns raised by the filtering and monitoring systems.

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). Staff may also use the NSPCC Whistleblowing Helpline.

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, NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to

behaviour which we consider is particularly concerning or breaks the law.

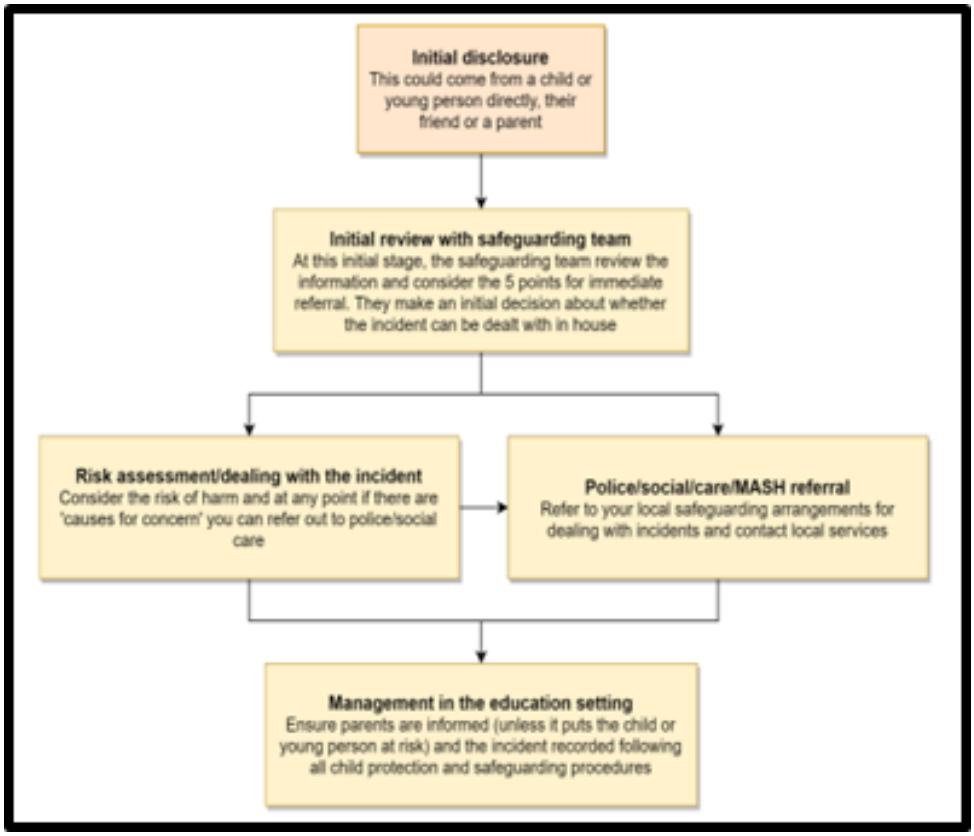
Nudes – sharing nudes and semi-nudes

All schools should refer to the UK Council for Child Internet Safety (UKCCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings.

There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all 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 school DSL will use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved.

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area. The UKCIS guidance seeks to avoid unnecessary criminalisation of children.



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.

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 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.

Where pupils 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 pupils) 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 cyber security

All pupils, 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
- 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 and daily backups taken off site, tapes rotation 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 – available to staff, students. Also available to 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

Data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in Data protection in schools, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2024, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Appropriate filtering and monitoring

The DSL has lead responsibility for filtering and monitoring and works closely with the IT department to implement the DfE filtering and monitoring standards, which require schools to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually

- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

We look to provide 'appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times.

We ensure ALL STAFF are aware of filtering and monitoring systems and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking.

Technical and safeguarding colleagues work together closely to carry out reviews and checks to ensure all systems are in operation and functioning as expected and also to ensure that the school responds to issues and integrates with the curriculum.

Safe Search is enforced on accessible search engines (Google and Bing) on all devices.

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. The school has also implemented Lightspeed Systems for additional filtering and monitoring to manage online learning and ensure student safety.

In addition to the LGFL and Lightspeed filtering system we use internally configured solutions (DNS, firewall) to provide more flexibility for teachers and use of digital resources.

According to the DfE standards, "a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

At Camden School for Girls we use a combination of all above options.

Messaging/commenting systems (incl. email, learning platforms)

- Pupils 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 pupils
- SecureEmail App, 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
- Pupils 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.

Use of generative AI

At Camden School for Girls, we acknowledge that generative AI platforms are becoming widespread. We are aware of and follow the DfE's guidance on this. In particular:

- In school, our AI policy provides guidelines for the ethical, secure and responsible use of Artificial Intelligence (AI) technologies. It is designed to provide a framework for the appropriate use of AI technologies while ensuring that students' privacy, security and ethical consideration are taken into account.
- The school blocks the generative AI 'bundle' on the filtering system and allows generative AI tools on a one-by-one basis where appropriate with limitations according to age or other factors.
- Our Digital Strategy Group is responsible for training staff in the use of generative AI and advises them on the appropriate use of AI tools for pedagogy including lesson planning and feedback.
- The process for approving the use of a new platform is overseen by the Head of ICT Support in collaboration with the Digital Strategy Group.
- In line with our AI policy, AI can be used as an aid for academic purposes, such as research, homework, and assignments, where permitted by the teacher. However, it is essential to note that students should not solely rely on AI to complete their work. The use of AI must be in line with academic integrity guidelines as outlined in the AI policy and JCQ guidelines AI Use in Assessments: Protecting the Integrity of Qualifications. Use of AI must be acknowledged and referenced.
- The school is committed to upholding academic integrity. Students are prohibited from using AI technologies to engage in cheating or plagiarism.
- Suspected breaches of academic integrity related to the use of AI technologies will be treated in line with our behaviour policy and / or examinations / non-examinations policies as appropriate. Any breaches of the policy will result in disciplinary action.

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 Juniper Education.

The Department for Education has determined information which must be available on a school website.

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

- School has 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)

Online storage or learning 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 pupils 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.

Any pupils 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 pupils, 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 pupils

Photos are stored on Shared Drive in Google Apps for Education in line with the retention schedule of the school Data Protection Policy or on the internal server 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).

Pupils 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.

Pupils 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.

Pupils 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.

The Headteacher updates schools' Twitter account.

Staff, pupils' and parents' SM presence

Social media (including 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 pupils 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, pupils and parents, also undermining staff morale and the reputation of the

school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13, but the school regularly deals with issues arising on social media with pupils/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 pupils/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). parentsafe.lgfl.net has helpful guidance and support for parents.

As outlined in the Acceptable Use Policies, pupils/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.

Pupils/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account) as laid out in the AUPs. 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 there has been a considerable number of Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital images and video. Parents must not covertly film or make recordings of any interactions with pupils or adults in schools or near the school gates, nor share images of other people's children on social media as there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of children for internal purposes such as recording attainment, but it will only do so publicly if parents have given consent on the relevant form.

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. Please see the Digital images and video section of this document for more information about filming and photography at school events. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office

Network / internet access on school devices/personal devices:

- Pupils/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 pupils/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 pupils/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.

Appendices

1. Safeguarding Incident log
2. Acceptable Use Policies (AUPs) for:
   - Pupils
   - Staff, Volunteers Governors & Contractors
   - Parents
3. Letter to parents about filming/photographing/streaming school events
4. E-Security Policy
5. Online-Safety Questions from the Governing Board (UKCCIS)
6. Education for a Connected World cross-curricular digital resilience framework (UKCCIS / UKCIS)
7. Sexting guidance from UKCCIS - Overview for all staff