E-Safety Policy

2025/2026

Approved by: Karen Pickles
Designated Safeguarding Lead
Date: 1st September 2025

POLICY REVISION RECORD (annual reviews)

Date	Section	Revision	Updated by
12/07/22	update KCSIE 2022	New policy in place	Karen Pickles
09/09/23	Re-written policy	Re-styled to include all above as required and KCSIE 2023	Karen Pickles
01/09/24		Reviewed	Karen Pickles
01/09/25		Reviewed and edited	Karen Pickles

www.berkeleyguardians.com
karen@berkeleyguardians.com
+44 (0) 7565493818

Aims and Objectives:

Whilst we would encourage all homestays to understand our aims and objectives; we also understand that Berkeley Guardians is not in place to educate the pupils in our care as a school is in place to do. What we aim to do is have an overall support for the pupils whilst they are in our care and the homestays to have an understanding as to how they can encourage positive use of devices and the internet.

- To protect and safeguard pupils in their use of ICT and e-technology
- To ensure pupils avoid infringing copyright, plagiarism or illegal downloading of music or video files
- To ensure pupils understand about unauthorised access to/loss of/sharing of personal information including personal data and images
- To raise awareness of and counter instances of cyberbullying. This includes bullying via text message, via instant-messenger services and social network sites, via email, and via images or videos posted on the internet or spread via mobile phone. It can take the form of any of the previously discussed types of bullying, i.e. technology can be used to bully for reasons of race, religion, sexuality, disability, etc.
- To encourage appropriate and very careful use of social networking sites or personal web pages and to know who to turn to report a concern
- To raise concerns regarding social media which are geared towards children. Whilst these are great platforms for communication they are also known for sharing of inappropriate personal data, explicit sexual talk/obscene language and this is likely to encourage inappropriate on-line contact with adults/strangers and potential or actual grooming from online predators. Internet offenders manipulate and target young people into criminal sexual activity.
- To ensure pupils using the internet in the homestay understand that excessive use may impact on the social and emotional development and learning of a young person.
- To ensure pupils online reputation is creditable and their digital footprint is viewed in a positive light.
- To ensure that pupils are aware of what 'Radicalisation' means and how pupils could be exposed to extremist material by accident, purposefully or by being targeted as stated in the Prevent Duty (2023)

Berkeley Guardians encourages pupils to use new and emerging technologies; which includes electronic tools or other such electronic devices, both fixed and mobile SMART devices, as they have important educational and social benefits.

Although pupils may be trusted by their parents regarding private internet use, Berkeley Guardians has a legal obligation to safeguard all pupils wherever possible when they are staying in our host families. We understand that their school will also do its utmost to prevent pupils from accessing material deemed unsuitable and/or in contravention of both the school's and Berkeley Guardians IT Acceptable Use Agreement.

As with any new technology, there are associated risks which include the following:

- exposure to inappropriate material
- physical danger
- online/cyberbullying

Introduction

Berkeley Guardians recognises the educational and social benefits that new and emerging technologies offer to young people. While our primary role is not to teach digital skills, we commit to supporting pupils in homestay placements by fostering safe, responsible and balanced use of devices and the internet.

1. Aims and Objectives

We aim to provide an overarching framework of support for pupils in our care and to equip homestays with the knowledge to encourage positive digital behaviours. Specifically, we will:

- Protect and safeguard pupils in their use of ICT and e-technology, both fixed and mobile.
- Prevent infringement of copyright, plagiarism or illegal downloading of music, video and software.
- Educate pupils about the risks of unauthorised access to, loss of, or sharing of personal information—including personal data and images.
- Raise awareness of cyberbullying across all channels: text, instant messaging, social networks, email and image/video sharing.
- Encourage careful and informed use of social networking sites and personal web pages, and clarify how to report concerns.
- Highlight the risks of child-focused social media platforms, including the sharing of explicit content, data exposure, and potential grooming by online predators.
- Advise on the impact of excessive internet use on social, emotional and academic development.
- Promote a positive digital footprint and reputation online.
- Ensure pupils understand “radicalisation” and recognise extremist material in accordance with the Prevent Duty.

2. Legislation and Guidance

This policy aligns with current statutory and best-practice frameworks. Key references include:

- Keeping Children Safe in Education (2023) and its 2024 addendum on online safety.
- Online Safety Act 2023, establishing duties for providers to manage harmful content.
- Age Appropriate Design Code (Children’s Code) 2020, regulating data collection from minors.
- UK Council for Internet Safety (UKCIS) guidance on filtering, monitoring and staff training.
- Counter-Terrorism and Security Act 2015 (Prevent Duty, updated 2024).
- Data Protection Act 2018 and General Data Protection Regulation (GDPR).
- National Cyber Security Centre (NCSC) “Cyber Security for Schools” guidance.
- DfE advice on cyberbullying, sexting and peer-on-peer abuse.
- CEOP (Child Exploitation and Online Protection) reporting protocols.

3. Roles and Responsibilities

- Designated Safeguarding Lead (DSL): Oversees online safety incidents, liaises with parents, schools and local authorities, and maintains policy review.
- Host Families: Implement filtering/monitoring measures, model safe online behaviour, report concerns promptly to the DSL.

- Parents/Guardians: Ensure personal devices are protected, supervise home network use, enforce parental controls and roaming data settings.
- Pupils: Follow the Acceptable Use Agreement (AUA), report any online concerns to host families or the DSL.
- Schools: Continue digital education in line with their AUA; collaborate with Berkeley Guardians on joint safeguarding measures.

4. Acceptable Use of ICT and Devices

1. Devices may only be used for lawful, age-appropriate and educational or social purposes that support a pupil's wellbeing.
2. Pupils must not access, create or share:
    - Illegal, extremist or explicit sexual content.
    - Unlicensed media (music, films, software).
    - Content that infringes privacy or defames individuals.
3. Social media and messaging:
    - Private accounts should have strict privacy settings.
    - Bullying, hate speech, grooming attempts or radical content must be reported immediately.
4. Emerging technologies:
    - Use of AI chatbots, virtual reality or wearable tech must follow homestay and school guidelines.
    - Pupils must not share personal data with unknown online services.

5. Filtering and Monitoring

- Host families must implement robust filtering at home (e.g., router-level, parental control apps) to block inappropriate sites.
- Monitoring should balance safeguarding with respect for pupils' privacy; alerts for risk categories (self-harm, radicalisation, sexual content) are essential.
- DSL will review filtering logs periodically and support host families in adjusting settings.

6. Education, Training and Awareness

- Homestay households receive annual training on online risks, updated each term to reflect new threats (e.g., deepfakes, phishing).
- Pupils will have access to age-appropriate e-safety resources and workshops, coordinated with their school.
- DSL circulates quarterly bulletins on emerging trends: AI misuse, social platform updates, gaming safety.

7. Responding to Incidents

- Any online safety concern must be reported immediately to the DSL.
- DSL logs incidents, conducts a risk assessment and liaises with parents, schools and external agencies (CEOP, police) as required.
- Where sexting or sexual imagery is involved, staff follow the UKCIS sexting guidance and local safeguarding protocols.

- Cyberbullying is addressed through pastoral support, mediation and, if necessary, referral to the school's disciplinary procedures.

8. Specific Online Risks

- Cyberbullying: Encourage bystander reporting, offer emotional support and mediation.
- Sexting: Educate on legal and emotional consequences; report all incidents to the DSL.
- Grooming and Radicalisation: Use Prevent Duty training to spot signs of targeted approaches; escalate concerns.
- Inappropriate Material: Maintain up-to-date filters; remind pupils of exit buttons/tools.
- Financial Scams & Gambling: Warn pupils about in-app purchases, loot boxes and unregulated platforms.

9. Device and Network Security

- Devices must run current antivirus/anti-malware software and the latest operating system updates.
- Host families are responsible for safeguarding guest devices; Berkeley Guardians and host families accept no liability for lost or damaged property.
- Public and home Wi-Fi networks should use WPA2/WPA3 encryption and strong passwords.

10. Parental Responsibilities

- Install and maintain parental controls on mobile data (4G/5G) and home broadband.
- Monitor data usage alerts to spot unusual patterns (streaming, downloads).
- Promote digital wellbeing: set screen-time limits, encourage regular offline activities.
- Reinforce policy expectations; collaborate with host families and the DSL on any concerns.

Cyber-Bullying

Cyber-bullying is defined as willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices.

Any host family or staff member who becomes aware of a pupil implicating themselves in cyber-bullying—whether as victim or perpetrator—must immediately contact the Designated Safeguarding Lead (DSL): Karen Pickles – karen@berkeleyguardians.com2

For further guidance on cyber-bullying, see "A Comprehensive Cyberbullying Guide for Parents" athttps://www.wizcase.com/blog/a-comprehensive-cyberbullying-guide-for-parents/

Pupil Code of Conduct

All pupils must agree to the Pupil Code of Conduct, which incorporates the IT Acceptable Use Policy. This document outlines:

- Permitted and prohibited uses of the host family's ICT network and devices
- Expectations around respect, privacy and copyright
- Reporting procedures for any online concerns

Pupils receive the Code of Conduct, Safeguarding leaflets and a Pupil Handbook on arrival in the UK. Compliance is a condition of their stay.

Designated Safeguarding Lead (DSL)

The DSL has overarching responsibility for all safeguarding and child-protection matters, including online safety. Responsibilities include:

- Reviewing and updating this policy annually
- Providing guidance and training to host families on ICT monitoring and support
- Logging and managing all online safety incidents, liaising with schools, parents and external agencies as required

Current DSL: Karen Pickles – karen@berkeleyguardians.com

Related Policies

- Anti-Bullying Policy
- Code of Conduct for Pupils
- IT Acceptable Use Policy
- Safeguarding and Child Protection Policy

Review and Continuous Improvement

- This policy is reviewed annually by the DSL to incorporate new legislation, technologies and safeguarding best practices.
- Feedback from pupils, host families and schools informs updates.
- Next scheduled review: August 2026.

Monitoring and Review

This section of the Online Safety Policy will be reviewed at least once every 12 months, incorporating updates to:

- Keeping Children Safe in Education (KCSIE) requirements
- Online Safety Act 2023 and subsequent regulations
- UK Council for Internet Safety (UKCIS) filtering and monitoring guidance

Next scheduled review: August 2026.

If you have feedback on this policy, please contact the DSL.

Further Considerations

- Introducing digital wellbeing check-ins at the start of each homestay term.
- Developing an interactive e-learning module on AI ethics and safe chatbot use.
- Providing homestays with a quick-reference “Online Safety Incident Flowchart.”
- Exploring collaboration with local youth services on cyber resilience workshops.
- Preparing for the UK Online Safety Bill’s implementation phases (due 2025–26).