



Richmond
Social Care Services

House
CIC

E-Safety Policy 2026 - 2027

Alternative Provision E-Safety Policy

1. Introduction

At Richmond House Social Care Services, we recognise the importance of providing a safe and secure online environment for all young people in our care. This E-Safety Policy outlines our commitment to safeguarding and promoting the welfare of children and young people who access our Alternative Provision (AP). The policy applies to all staff, students, volunteers, and visitors and ensures that everyone understands their roles and responsibilities in maintaining e-safety.

This policy is written in accordance with Keeping Children Safe in Education (KCSIE) 2026, which comes into force on 1 September 2026, the Data Protection Act 2018, and other relevant legislation and guidance. The 2026 edition of KCSIE contains a number of significant changes, ranging from staff training requirements and safer recruitment practices to online safety, artificial intelligence (AI), and child-on-child abuse.

2. Aims

- To safeguard children and young people from potential online harms, including emerging risks such as AI-generated content and deepfakes.
- To educate children and young people about e-safety and responsible internet use.
- To establish clear guidelines and procedures for online activities.
- To provide training and support for staff on e-safety issues, including understanding filtering and monitoring systems.
- To ensure compliance with legal requirements and best practices in e-safety.
- To ensure that the effectiveness of filtering and monitoring systems is reviewed at least once every academic year.

3. Roles and Responsibilities

Senior Leadership Team:

- Ensure the implementation and regular review of the E-Safety Policy.
- Allocate appropriate resources for e-safety initiatives and training.
- Ensure that an SLT member is named and responsible for filtering and monitoring reviews.
- Ensure that filtering and monitoring reviews are documented and evidenced.

E-Safety Coordinator:

- Oversee the implementation of e-safety practices.
- Provide training and support to staff and students.
- Monitor e-safety incidents and maintain records.

Designated Safeguarding Lead (DSL):

- The DSL's role must explicitly include understanding filtering and monitoring systems and processes.

- Support the SLT member responsible for filtering and monitoring in conducting annual reviews.
- Ensure that safeguarding training for all staff includes an understanding of filtering and monitoring expectations and how concerns should be escalated.

Staff:

- Adhere to the E-Safety Policy and guidelines.
- Educate and supervise students during online activities.
- Report any e-safety concerns or incidents to the E-Safety Coordinator or DSL.
- **All staff must now read Part One of KCSIE 2026 in full** – the condensed version previously found in Annex A has been removed.

Students:

- Follow the e-safety guidelines provided by the staff.
- Report any e-safety concerns to a trusted adult.

Parents/Carers:

- Support the centre's e-safety initiatives.
- Encourage responsible online behaviour at home.

4. E-Safety Education and Training

For Students:

- Regular e-safety lessons integrated into the curriculum, using age-appropriate resources such as CEOP Thinkuknow.
- Workshops and activities focused on responsible internet use, cyberbullying, and online privacy.
- Education on **AI-generated content and deepfakes**, including how to recognise and respond to them.
- Access to resources and support for dealing with online issues.
- The **UKCIS "Education for a Connected World"** framework underpins our approach, covering eight key areas: self-image and identity, online relationships, online reputation, online bullying, managing online information, health, wellbeing and lifestyle, privacy and security, and copyright and ownership.

For Staff:

- Mandatory e-safety training during induction and regular updates, including training on filtering and monitoring expectations and the 4Cs framework (Content, Contact, Conduct, Commerce).
- Access to resources and support for managing e-safety in the classroom.
- Training on emerging risks including AI, deepfakes, and generative AI.
- Understanding of the updated online risk categories in KCSIE 2026.

For Parents/Carers:

- Information sessions and workshops on e-safety.
- Guidance on monitoring and supporting children's online activities at home, including awareness of AI-generated content risks.

- Signposting to resources such as UK Safer Internet Centre and CEOP Thinkuknow.
-

5. Safe Use of Technology

Internet Access:

- Supervised and filtered internet access for students.
- Use of secure and monitored network connections.
- Filtering and monitoring systems must be reviewed for effectiveness at least once every academic year and records of these reviews must be kept.
- Reviews must include checks that filtering works appropriately across all internet-connected devices in all relevant locations.

Devices:

- Guidelines for the safe use of school-provided devices.
- Restrictions on the use of personal devices during school hours unless authorised.
- In line with KCSIE 2026, we operate a mobile-phone-free environment during the school day.

Social Media:

- Education on the risks and responsible use of social media.
- Monitoring and guidance on appropriate social media interactions.

Artificial Intelligence (AI):

- Staff and students must be aware of the risks associated with AI-generated content, including deepfakes.
 - The DfE's guidance on "Generative AI: product safety expectations" informs our approach to filtering and monitoring in relation to generative AI within educational settings.
 - Updated terminology now refers to "nudes" rather than "sexting" or "indecent images", which includes digitally-altered images including AI-generated or altered images and deepfakes.
 - Staff must be aware of the risks of unsupervised interactions with AI systems.
-

6. Implementation of YouTube Kids

Richmond House has successfully established and completed the implementation of YouTube Kids to ensure that children's access to content is limited, monitored, and age-appropriate. The following measures are now in place:

1. **Individual Accounts:** Each child has their own YouTube Kids account tailored to their learning and developmental needs, allowing for personalised content recommendations based on age and interests.
2. **Content Filtering:** We have configured the filtering options on YouTube Kids to ensure that the videos available are suitable for each child's age group, effectively restricting access to inappropriate content.
3. **Monitoring Usage:** Educators and caregivers are regularly monitoring each child's viewing history to ensure compliance with our E-Safety standards. This includes reviewing the types of content accessed to ensure alignment with educational goals.

4. **Time Limits:** Guidelines have been established for the amount of time children can spend on YouTube Kids, promoting a balanced approach to screen time and encouraging other forms of learning and interaction.
5. **Parental Involvement:** We've actively engaged parents and guardians in their children's online activities, providing regular updates about the content their children are viewing and recommendations for suitable educational resources.
6. **Feedback Mechanism:** A feedback mechanism is now in place for educators and parents to report any concerns regarding the content accessed through YouTube Kids, allowing us to promptly address any issues and adjust our monitoring practices as necessary.
7. **Education on Online Safety:** Children are receiving guidance on online safety and digital citizenship, helping them to understand the importance of safe and responsible internet use.

Through the successful implementation of these measures, we aim to create a safe and enriching online environment for children, facilitating their learning and development while ensuring their safety and well-being.

7. Reporting and Responding to E-Safety Incidents

Incident Reporting:

- Clear procedures for reporting e-safety concerns or incidents.
- Anonymous reporting options for students.
- All staff must be aware of how to escalate concerns, including through filtering and monitoring systems.

Incident Response:

- Immediate action to address and resolve e-safety incidents.
 - Support for affected individuals and appropriate disciplinary measures if necessary.
 - Recording and monitoring of incidents to identify trends and inform future e-safety strategies.
 - Where incidents involve AI-generated content or deepfakes, specific procedures apply in line with KCSIE 2026 guidance.
-

8. Monitoring and Review

Regular Monitoring:

- Continuous monitoring of e-safety practices and incidents.
- Regular feedback from students, staff, and parents/carers.

Filtering and Monitoring Reviews:

- **Annual reviews** of filtering and monitoring systems must be conducted, led by the SLT member responsible, with support from the DSL and IT support.
- Records of these reviews must be kept, documenting when checks were conducted, which devices and environments were tested, identified issues, and actions taken to address concerns.

Policy Review:

- Annual review of the E-Safety Policy by the Senior Leadership Team and E-Safety Coordinator.
- Updates to the policy based on emerging risks, technological changes, and feedback.
- The policy and its implementation will be reviewed annually, or sooner if required due to changes in legislation.

9. Legal Framework and References

- Compliance with the **Data Protection Act 2018** and **UK GDPR**.
- Adherence to the **Children Act 1989 and 2004**.
- **Keeping Children Safe in Education (KCSIE) 2026** – comes into force on 1 September 2026.
- **Working Together to Safeguard Children (2026)** – updated on 18 March 2026, replacing the 2023 version.
- **UKCIS "Education for a Connected World"** framework.
- **CEOP Thinkuknow** resources.
- **UK Safer Internet Centre** guidance on filtering, monitoring, and image security.
- **DfE Filtering and Monitoring Standards** (updated June 2026).
- **DfE Generative AI in Education** guidance.

10. Summary of Key KCSIE 2026 Changes Relevant to E-Safety

Change	Implication for Richmond House
Annex A removed	All staff must read Part One in full
Annual filtering and monitoring reviews	SLT member must lead and document annual reviews
AI and online safety	Policies must address AI-generated content, deepfakes, and generative AI risks
Updated terminology ("nudes")	Policies and training must use updated language
Mobile-phone-free environment	Implement restrictions on mobile phone use during the school day
Greater emphasis on alternative provision	Enhanced safeguarding due diligence for AP placements
Updated 4Cs framework	Online risk categories updated with new content risks
DSL responsibilities	DSL must understand filtering and monitoring systems
Staff training	Must include filtering, monitoring, and escalation procedures
Record-keeping	Records of filtering checks must be kept

Richmond House Social Care Services is committed to providing a secure and supportive online environment for all young people in our care. Through education, supervision, and clear policies, we aim to equip our students with the knowledge and skills they need to navigate the digital world safely and responsibly.

Approved by:

Jay Al Karaki

Senior Leadership Team

Date:

01/09/2026

Review Date:

September 2027

Document Version: Vr 08

Review Period: 2026 – 2027