# ONLINE SAFETY POLICY

| | | | |
|---|---|---|---|
| ORGANISATION | SKAPE North East Ltd | POLICY REFERENCE | P10 |
| UPDATED | 12 November 2026 | NEXT SCHEDULED REVIEW | 12 November 2027 |
| POLICY OWNER | Centre Manager / DSL | RELATED POLICIES | Safeguarding; Handheld Device and Mobile Phone; GDPR, Safe Gaming |

## 01 INTRODUCTION

The internet and digital technology are an important part of everyday life and education. They provide opportunities for learning, communication, creativity and independence. SKAPE recognises that children and young people must be supported to use technology safely, securely, responsibly and critically, and must know how to seek help if something goes wrong.

## 02 SCOPE AND SAFEGUARDING RESPONSIBILITIES

This policy supports and complements SKAPE's safeguarding arrangements and reflects Keeping Children Safe in Education (KCSIE) 2026. It applies to all members of the SKAPE community, including students, staff, directors, visitors and volunteers.

Commissioning schools retain overarching safeguarding responsibility for students placed with SKAPE. SKAPE remains responsible for safeguarding students while they attend. We will follow our own Safeguarding Policy alongside the relevant commissioning school or local authority's safeguarding procedures. Our DSL will liaise with their DSL or safeguarding contact about online concerns and share relevant information. Urgent safeguarding action must not wait for a response from the commissioner.

## 03 TEACHING AND LEARNING

**Why the internet and digital communications are important**

- Internet access and digital technology are important learning tools and may be used to enhance and extend teaching, learning and independence.
- Clear boundaries will be set for appropriate use of the internet, digital communications, devices and online services, and these will be discussed with staff and students.
- Students will be taught to locate, retrieve and evaluate information, including how to identify misinformation, disinformation, manipulated content and unreliable sources.
- Students will be supported to understand copyright, intellectual property and responsible use of online material.

**Usernames and passwords**

- Student access to SKAPE internet-connected devices will be appropriately controlled. Passwords and account credentials must not be shared unless an authorised arrangement is required for safeguarding, accessibility or supervision.
- Where staff log a student into a device or service, use will be supervised and screens positioned, where practicable, so activity can be monitored appropriately.

## 04 STAFF RESPONSIBILITIES

- All staff must understand that online safety is part of safeguarding and must follow SKAPE's safeguarding and reporting procedures when concerns arise.

- Relevant staff must understand how SKAPE's filtering and monitoring arrangements operate, what their role is, and how to report or escalate concerns.
- Staff must maintain professional boundaries in all digital communication with students and must only use approved channels for educational or safeguarding purposes.

## 05 FILTERING AND MONITORING

SKAPE will do all that it reasonably can to limit children's exposure to harmful or inappropriate online content through the provision's IT systems. Appropriate filtering and monitoring arrangements will be in place and will be proportionate to the age, needs and vulnerability of students, the nature of the provision, how technology is used and the safeguarding risks identified.

- The Centre Manager and DSL oversee online safety, including filtering and monitoring. The Centre Manager coordinates technical support, while the DSL leads on safeguarding concerns.
- Staff must report technical problems or online safety concerns promptly to the Centre Manager or DSL. Specialist IT support will be sought where needed to set up, check or resolve technical issues.
- Filtering and monitoring provision will be formally reviewed at least once every academic year and following significant changes to systems, risks or provision.
- Checks will include whether filtering operates appropriately on internet-connected devices and in relevant locations used by students. A record of checks and reviews will be retained.
- Filtering will block harmful and inappropriate content without unreasonably affecting teaching and learning. Monitoring strategies will reflect SKAPE's safeguarding needs.
- Safeguarding alerts, concerns or attempted access to harmful content will be reviewed and escalated in accordance with SKAPE's Safeguarding Policy.
- Filtering and monitoring arrangements will be informed by relevant risk assessments, including Prevent-related risks where applicable, and by DfE filtering and monitoring standards.

Students and staff will be informed, in an age-appropriate and transparent way, that use of SKAPE networks and devices may be monitored. Any personal data generated through monitoring will be handled in accordance with UK GDPR, the Data Protection Act 2018, as amended, and SKAPE's data-protection arrangements.

The Centre Manager/DSL will make sure staff know who checks alerts, how quickly concerns must be acted on and who provides cover. Staff must know when monitoring is not active.

## 06 UNDERSTANDING ONLINE RISKS

KCSIE 2026 identifies online safety as an integral part of safeguarding. Online harm may occur alongside other forms of abuse and may take place wholly or partly online. SKAPE will address online risks through safeguarding practice, curriculum activity, staff training and appropriate technical controls.

Students will be educated, at an appropriate level, about the four broad areas of online risk:

- Content - being exposed to illegal, inappropriate or harmful content, including misinformation, disinformation and conspiracy theories.
- Contact - harmful online interaction with adults, peers or AI applications that simulate a relationship or conversation.
- Conduct - personal online behaviour that increases the likelihood of, or causes, harm, including sharing explicit or AI-generated sexual images and online bullying.
- Commerce - risks such as online gambling, inappropriate advertising, phishing, scams and other financial harms.

Students will be taught how to protect themselves and others, how to report concerns, and where to access support. Any safeguarding concern relating to online activity must be managed under SKAPE's Safeguarding Policy (P01).

## 07 MANAGING INTERNET ACCESS

**Information system security**

- The Centre Manager will arrange regular reviews of SKAPE's ICT security, with specialist IT support where needed.
- Supported devices and software will be maintained with appropriate security updates, malware protection and access controls.
- Cyber-security concerns will be reported promptly and managed in line with DfE cyber-security standards and SKAPE's internal procedures.

**Email**

- Students will not routinely be provided with SKAPE email addresses. Access to personal email accounts on SKAPE systems may be restricted where this is necessary for safeguarding, security or learning purposes.

**Published content and the SKAPE website**

- Personal contact information for staff or students will not normally be published. Official SKAPE contact details will be used for public communication.
- Published content will be accurate, appropriate and authorised by a designated member of staff.

**Publishing students' images and work**

- Images of students will be selected and used carefully, with consideration given to safeguarding, privacy and the risk of misuse.
- Students' full names will not normally be published alongside photographs or other identifying content.
- Written parent/carer consent and, where appropriate, student agreement will be obtained before identifiable images or student work are published, in line with SKAPE's GDPR Policy. For students aged 18 or over, staff must follow the consent arrangements that apply to the student.

Staff must use authorised SKAPE equipment for student photographs, video and audio, and follow the Handheld Device and Mobile Phone and GDPR policies for consent, storage and sharing.

## 08 SOCIAL NETWORKING AND PERSONAL PUBLISHING

- SKAPE will control or restrict access to social-networking services where appropriate and will educate students about safe and responsible use.
- Students will be advised not to disclose personal information that could identify themselves, other people or their location.
- Students will be taught to consider privacy, permanence and potential misuse before sharing images or other content online.
- Students will be encouraged to use appropriate privacy and security settings, strong passwords and blocking/reporting tools.
- Staff must not use personal social-media accounts to communicate with students and must maintain appropriate privacy settings and professional boundaries.

## 09 EMERGING TECHNOLOGIES AND PERSONAL DEVICES

New and emerging technologies will be considered for educational benefit and appropriately risk assessed before being introduced for student use. This includes consideration of safeguarding, filtering and monitoring, privacy, data protection, security, accessibility, age restrictions and the needs of students with SEND.

**Mobile phones and personal devices**

Mobile phones and other personal devices are governed by SKAPE's Handheld Device and Mobile Phone Policy. SKAPE is phone-free by default throughout the student day. Any individual exception must be agreed under that policy, including medical and accessibility needs. Learning activities will normally use SKAPE devices.

## 10 GENERATIVE ARTIFICIAL INTELLIGENCE

SKAPE recognises that generative AI can support education but may also create safeguarding, privacy, accuracy, intellectual-property and developmental risks. Use of generative AI will therefore be planned, proportionate and subject to appropriate oversight.

- Only AI tools considered appropriate for the intended educational purpose and user group should be used with students. Relevant age restrictions and provider terms must be observed.
- Student-facing AI tools will be considered against DfE generative AI product safety standards, including filtering, monitoring, security, privacy, data protection and safeguarding features.
- Staff and students must not enter identifiable, confidential or special-category personal data into public or unapproved AI systems unless the use has been specifically authorised and relevant data-protection requirements have been addressed.
- AI-generated material must not automatically be treated as accurate. Staff and students will be encouraged to check accuracy, sources, bias and appropriateness.
- Student use of AI will be supervised and monitored where appropriate. Any disclosure or content suggesting a safeguarding concern must be reported through normal safeguarding procedures.
- AI tools introduced for regular or higher-risk use will be risk assessed. Where personal-data processing is likely to result in high risk, a Data Protection Impact Assessment (DPIA) must be completed before use.
- Teaching about AI will include critical digital literacy, responsible use, academic integrity and the importance of maintaining independent thinking and learning.

## 11 PROTECTING PERSONAL DATA

- Personal data will be collected, processed, stored, transferred and disposed of in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, as amended, and SKAPE's data-protection arrangements.
- Personal or confidential data must not be stored on removable media unless this is authorised and appropriately protected, for example through encryption and access controls.
- Where monitoring technology processes personal data, SKAPE will be transparent about its purpose and access arrangements and will apply appropriate retention and security controls.
- A DPIA must be completed before introducing new technologies or monitoring arrangements where the processing is likely to result in a high risk to individuals' rights and freedoms.

## 12 INTERNET ACCESS AND RESPONDING TO CONCERNS

### Authorising internet access

- All staff must comply with SKAPE's Employee Code of Conduct and relevant ICT/acceptable-use requirements before using SKAPE ICT resources.
- SKAPE will maintain appropriate records of authorised access to its systems and accounts.
- Students will be expected to follow SKAPE's Responsible Internet Use expectations and any individual arrangements established for their placement.

### Assessing risks

- SKAPE will take reasonable and proportionate precautions to prevent access to harmful or inappropriate material. No technical system can eliminate all online risk, so technical controls will operate alongside supervision, education and safeguarding procedures.
- ICT use, filtering and monitoring arrangements, and implementation of this policy will be reviewed to ensure they remain appropriate and effective.

### Handling online-safety concerns and complaints

- Concerns about student internet misuse will be managed by an appropriate senior member of staff under the Behaviour and No Bullying policies. Any safeguarding concern must be reported immediately to the DSL.

- Concerns or allegations involving staff must be managed in accordance with SKAPE's safeguarding, staff conduct and allegations procedures, including referral to the appropriate senior person or external authority where required.
- Potentially illegal online activity must be reported promptly to the DSL. Preserve evidence safely, without copying or circulating harmful images. Advice may be sought from the police, CEOP, local authority or other relevant agencies.
- Students and parents/carers will be informed about reporting routes under the Safeguarding and Complaints policies. Staff can also raise concerns through the Whistleblowing Policy.

If a concern involves nude or semi-nude images of a child, staff must not deliberately view, copy, screenshot, save, forward or delete them, or ask a student to do so. Report immediately to the DSL, who will follow UKCIS guidance. If seen accidentally, stop viewing and tell the DSL. Staff must not investigate or search a student's device themselves.

## 13 COMMUNICATING ONLINE SAFETY

- Age-appropriate online-safety expectations will be communicated to students and reinforced through teaching, induction and day-to-day practice.
- Students will be informed that use of SKAPE networks, systems and devices may be filtered and monitored.
- Online safety, digital literacy, misinformation, AI awareness and critical evaluation of online content will be addressed through relevant curriculum and PSHE/RSHE activity.

**Staff and the Online Safety Policy**

- All staff will have access to SKAPE's Safeguarding and Online Safety policies and will be expected to understand their responsibilities.
- Staff with specific filtering or monitoring responsibilities will receive appropriate information, support and training and will follow clear escalation procedures.
- SKAPE-provided IT equipment remains the property of SKAPE and must be used for authorised purposes.

**Parents and carers**

- Parents' and carers' attention will be drawn to SKAPE's Online Safety Policy through appropriate communication and/or the SKAPE website.
- SKAPE will signpost parents and carers to appropriate online-safety information and support where relevant.

## 14 RELATED POLICIES

Read alongside SKAPE's Safeguarding, Handheld Device and Mobile Phone, Employee Code of Conduct, Behaviour, No Bullying, Confidentiality, GDPR, Visitor, Complaints and Whistleblowing policies, and relevant acceptable or responsible use agreements.

## 15 RELEVANT LEGISLATION AND GUIDANCE

- Further support: UK Safer Internet Centre (saferinternet.org.uk) and CEOP Education (ceopeducation.co.uk).
- Department for Education, Keeping Children Safe in Education 2026 (in force from 1 September 2026).
- Department for Education, Filtering and monitoring: core standard, Meeting digital and technology standards in schools and colleges (updated 16 September 2026).
- Department for Education, Cyber security: core standard, Meeting digital and technology standards in schools and colleges (updated 16 September 2026).
- Department for Education, Generative AI: product safety standards (updated 19 January 2026).
- UK Council for Internet Safety, Sharing nudes and semi-nudes: advice for education settings (updated 11 March 2024).
- UK GDPR and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025.

## 16 MONITORING AND REVIEW

The Centre Manager/DSL will review this policy annually, or sooner if guidance, technology or SKAPE's arrangements change. Reviews will consider online concerns, filtering and monitoring checks, and feedback from staff, students and families.

## 17 DOCUMENT REVISION HISTORY

| DATE | CHANGE | APPROVAL | REV. |
|---|---|---|---|
| 10/08/2023 | Initial policy | K. Watson | 01 |
| 11/09/2023 | Amendments to reflect KCSIE guidance | K. Watson | 02 |
| 31/08/2024 | Policy review and KCSIE updates | K. Watson | 03 |
| 04/09/2025 | Policy review and KCSIE updates | K. Watson | 04 |
| 23/09/2026 | Updated for KCSIE 2026, filtering and monitoring, data protection, mobile devices and generative AI guidance | K. Watson | 05 |
| 12/11/2026 | Branding and layout standardised; brief updates to align related policies. Technical support responsibilities clarified and guidance dates checked. | D. James | 06 |