GENERAL INTRODUCTION

The internet has grown exponentially since its inception. It is part of everyday life and an important tool to use and embrace. The internet offers great solutions for everyday problems and is widely used for education, entertainment and social networking. In the classroom it is used to enhance our children's learning and encourages independence for them to explore and discover new things.

We need to make sure that we support our children while using the internet to make sure they are accessing it in a safe, secure and knowledgeable way. So that if anything were to go wrong then they would know how to react and resolve the situation.

Please see the links below for further guidance on safe usage of the internet:

www.thinkuknow.co.uk

www.saferinternet.org.uk

www.ceop.police.uk/safety-

THE E-SAFETY POLICY

This policy supports and compliments provisions safeguarding policy, reflecting statutory requirements under KCSIE 2025. It applies to all members of the SKAPE community, including students, staff and volunteers.

The commissioning school places children in alternative provision, where safeguarding remains the responsibility of the school. Thorough checks of SKAPE's safeguarding procedures and policies will be carried out by commissioning schools.

TEACHING AND LEARNING

Why the Internet and digital communications are important.

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with high-quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.

Internet use will enhance and extend learning.

- Clear boundaries are set for the appropriate use of the Internet and digital communications and discussed with both staff and students. Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Students will be taught how to evaluate Internet content.

The e-Safety co-ordinator, where possible, will ensure that the use of Internet derived materials by both staff and students complies with copyright law. Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Usernames and passwords

- The Centre's internet access will only be accessible to students once a member of staff has logged in for them via a secure password. Whilst using the internet, the orientation of students seating/desks will be such that the screens of computers will be visible to staff at all times and their work will be supervised and closely monitored.

STAFF RESPONSIBILITIES

- Both staff and managers must understand how filtering and monitoring systems operate, be able to manage them effectively and know how to escalate concerns. www.saferinternet.org.uk

FILTERING AND MONITORING RESPONSIBILITIES

Whilst considering our responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, SKAPE will be doing all it reasonably can to limit children's exposure to risks from the centre's IT system.

As part of this process, SKAPE will ensure it has appropriate filtering and monitoring systems in place and will regularly review their effectiveness. We will ensure that senior and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

If it is necessary, we will pursue training in this area and take advice from experts or services that are designed to help.

Keeping children safe in education 2025

These standards, which are highlighted in KCSIE 2025, build on and reinforce the importance of filtering and monitoring as part of a more strategic approach for online safety. Key Changes in KCSIE 2025 emphasise strengthened filtering and monitoring systems and there are clearer requirements regarding filtering and monitoring technologies. The guidance encourages the use of the Department for Education's "Plan Technology for Your School" tool to assess and improve filtering and monitoring standards. Plan technology for your school - GOV.UK

SKAPE will consider the number of and age range of our children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

We will assess the appropriateness of any filtering and monitoring systems used in SKAPE and this will be informed, in part, by the risk assessment required by the Prevent Duty.

The DSL will undertake the responsibility to ensure that this duty is carried out and will follow the guidance in the KCSIE 2025 update, along with the support of the LA, if needed.

SKAPE's IT Lead will also support in this role.

To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools and colleges should:

• *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. Governing bodies and proprietors should review the standards and discuss with IT staff and service providers what more needs to be done to support schools and colleges in meeting this standard.*

Additional guidance on "appropriate" filtering and monitoring is given in the KCSIE 2025 document, paragraphs 141-148 and in Annex B and should be read along with this section of the policy. Please see the link below:
Keeping children safe in education 2025

The DfE has also published guidance on the features that Generative AI systems should meet, to be considered safe for users in educational systems. The guidance explains how filtering and monitoring requirements apply to the use of generative AI in education. Further information can be found here:
Generative AI: product safety expectations - GOV.UK

ONLINE SAFETY

KCSIE 2025 guidance highlights online safety as a core safeguarding concern, recognising that online abuse often occurs alongside offline abuse. Schools are now required to address online risks separately from offline abuse, ensuring comprehensive safeguarding practices.

As part of the Centre's PSHE/RSHE programme, students will be educated on how to recognise online abuse, and the four areas of risk to online safety:

Content - (misinformation/disinformation and conspiracy theories)
Contact - being subjected to harmful online interaction with other users
Conduct - online behaviour that increases the likelihood of, or causes, harm
Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams

To address the challenges posed by the digital landscape, SKAPE will take an active approach in educating students on how to safeguard themselves and others against these risk, and provided with information on where to access support. Staff are required to follow SKAPE's Safeguarding Policy (P01) should any concerns arise pertaining to a student's online safety. Further information on online safety advice can be found in Annex B of the KCSIE 2025 guidance (P166-167).

MANAGING INTERNET ACCESS

Information system security

Updates within KCSIE 2025 clarify the DfE's cyber security standards and advise that schools take appropriate actions to meet these standards to enhance resilience against digital threats. Further information can be found here: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges

- SKAPE's ICT system security will be regularly reviewed by the centres IT lead.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed, where necessary, at the centres staff meetings.

E-mail

Students will not be provided with email addresses and will be prohibited from accessing their personal emails.

Published content and the school website.

- Staff or student personal contact information will not generally be published.
- The contact details given online should be the school office.
- The e-Safety coordinator responsible for ICT will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Publishing students' images and work

- Photographs that include students will be selected carefully so that individual students cannot be identified, or their image misused.
- Students' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website (see Safeguarding policy- P01).
- Work can only be published with the permission of the student and parents/carers.

Social networking and personal publishing

- SKAPE will control access to social networking sites and will educate students in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Students should not place personal photos on any social network space without considering how the photo could be used now or in the future.
- Students should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others.

Managing filtering

- SKAPE will work with the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the e-Safety Coordinator or a senior member of staff.

- The e-Safety coordinator responsible for ICT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

MANAGING EMERGING TECHNOLOGIES

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time unless for a specific reason and then under the direct supervision of a member of staff. The sending of abusive or inappropriate text messages is forbidden.
- The use by students of cameras in mobile phones will not be permitted in school.
- Student Internet access via mobile phone is not permitted in SKAPE.

PROTECTING PERSONAL DATA

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- No student/staff personal data must be stored on any removable device unless encrypted / pass worded.

POLICY DECISIONS

Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.
- Staff must ensure that a signed copy of the agreement is in the possession of the eSafety co-ordinator. The school will maintain a current record of all staff and students who are granted access to school ICT systems.
- All students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement.

Assessing risks

- SKAPE will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network.
- SKAPE cannot accept liability for any material accessed, or any consequences of Internet access.
- SKAPE will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the centre manager.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures (see safeguarding policy).
- Students and parents will be informed of the complaints procedure.

- Discussions will be held with the Police to establish procedures for handling potentially illegal issues.

Communicating e-Safety

- E-Safety rules will be posted in all rooms where students will be accessing computers.
- Students will be informed that network and Internet use will be monitored.
- A programme of training in e-Safety will be included in the IT Induction lessons at KS3 and KS4.

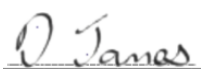
Staff and the e-Safety policy

- All staff will be given the SKAPE Safeguarding and e-Safety Policy, and its importance explained.
- Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.
- The internet should only be used in the Centre where the individual's specific use is necessary to enable them to carry out their work in school.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Training will be provided on new content risks, AI awareness and monitoring responsibilities.
- Digital literacy/ PSHE lessons will address misinformation, AI and critical evaluations of online content.
- Staff should ensure that any IT equipment provided by SKAPE remains the property of the school at all times and should only be used for the purpose(s) it is intended for.
- Staff should understand that phone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship and should not communicate online with students in any way other than for school purposes – e.g., for the submission of assignments etc.
- Staff should not use Facebook or any other social networking site to communicate with students. They must ensure that the use of Facebook etc is restricted so that pupils cannot gain access to their profile.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the SKAPE's e-Safety Policy in meetings and on the website.
- SKAPE will maintain a list of e-safety resources for parents/carers.

This policy reflects the strengthened emphasis in KCSIE 2025 on digital safeguarding and preparedness for evolving technology risks, ensuring SKAPE maintains a safe, responsive and proactive approach to e safety.

Signed:  Date: 04/09/2025

Print Name: D. James
Reviewed: Annually
Review Date: September 2026

Date	Reason for Change	Approved By	Revision Number
10/08/23	Initial Policy	K Watson	Rev 1
11/09/23	Amendments made to reflect KCSIE Guidelines	K Watson	Rev 2
31/08/24	Policy Review- Updates included to reflect current KCSIE Guidelines	K Watson	Rev 3
04/09/2024	Policy Review- Updates included to reflect current KCSIE Guidelines	K Watson	Rev 4