

Policy owner	Shane Edwards, Senior Assistant Head
Approval	Local Advisory Committee / Trust approval
Implementation date	September 2026
Review date	September 2027

SOUTHVIEW SCHOOL, COLLEGE & THE VIEW

E-Safety Policy

Hereafter referred to as “Southview School”

Writing and reviewing the E-safety Policy

The E-safety Policy is part of the School Monitoring and review Schedule and relates to other policies including those for computing education, anti-bullying and for child protection.

The school has appointed the **Headteacher** to be responsible for ensuring e-safety is embedded in the school's safeguarding culture and that appropriate training and policies are implemented. Responding to online safeguarding incidents (as detailed in KCSIE 2026), will be the responsibility of the school's Designated Safeguarding Lead (DSL) and appointed deputies.

The E-safety Policy and its implementation will be reviewed annually.

This policy applies to any person using ICT on school premises including (but not limited to) pupils, staff, volunteers, Ambassadors, parents, carers and visitors.

All staff members must read Part 1 of Keeping Children Safe in Education 2026 in full as part of their induction and annually thereafter.

Teaching and learning:

As an aspirational school for students with Physical and Neurological Impairments (PNI), all teaching and learning is adapted to allow students to access information where possible, in relation with their neurological development.

Why 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 quality internet access as part of their learning experience.

Pupils will cover the eight different aspects of the Education for a Connected World framework.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Currently, the school internet access is provided by LGFL (London Grid for Learning) through a regional broadband contract, which includes filtering appropriate to the age of pupils.

Access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate internet content

The school will seek to ensure that the use of internet derived materials by staff and by pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils will be taught how to report unpleasant internet content e.g. telling a responsible adult.

For pupils whose parents lack economic or cultural educational resources, the school should build digital skills and resilience acknowledging the lack of experience and internet at home.

Pupils will be educated about the risks associated with generative AI tools, including:

- How AI can be used to create inappropriate or harmful content
- The importance of critically evaluating AI-generated information
- How to use AI tools safely and responsibly
- Understanding that AI-generated images and content may not be real

Managing internet Access Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.
- The school's filtering and monitoring systems apply to all internet access, including access to generative AI tools used for educational purposes.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system (where they are set up) for matters related to school.
 - Pupils/parents/carers must immediately tell a teacher if they receive offensive e-mails linked to school.
 - Staff to pupil/parent/carer email communication must only take place via a school email address and will be monitored except when the pupil is known to the member of staff in a capacity other than through school e.g. if a member of staff has a child at the school they may have other parents' details in order to arrange play dates.
 - Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
 - The forwarding of chain letters is not permitted.
 - Cc/Bcc or inform Headteacher of any e-mail deemed sensitive.
-

Published content and the school website

The contact details on the website should be the school address, e-mail and telephone number.

The Senior Assistant Headteacher, School Business Manager and Finance Assistant will take overall editorial responsibility and ensure that content is accurate and appropriate. Hope Academy Trust will take overall responsibility for ensuring the necessary compliance for the website.

Publishing pupils' images and work

Photographs that include pupils will be selected carefully.

Pupils' full names will be avoided on the website as appropriate, included in blogs, forums or wikis, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Making or Sharing of Nudes or Semi-Nudes (including AI-generated images)

The school recognises that the making or sharing of nudes or semi-nudes by children is a safeguarding issue and all incidents will be managed accordingly.

This includes:

- Images or videos where a child is naked, partially naked, or in their underwear
- Images or videos that have been digitally altered or manipulated
- Images or videos that are wholly generated by artificial intelligence (AI), including deepfakes

All incidents involving the making or sharing of nudes or semi-nudes require a safeguarding response, regardless of whether the content was created or shared consensually.

Staff will:

- Never view, copy, print, share or save the imagery
- Report the incident immediately to the DSL or a deputy DSL
- Confiscate the device involved and secure it
- Follow the school's child protection procedures

The DSL will:

- Hold an initial review meeting to establish the facts and assess risks
- Decide on appropriate next steps in line with UKCIS guidance "Sharing nudes and semi-nudes: advice for education settings working with children and young people"
- Consider whether the incident should be reported to police and/or children's social care
- Record all decisions and actions taken
- Ensure appropriate support is provided to all children involved

Pupils will be educated about:

- The serious consequences of making or sharing nudes or semi-nudes
 - The permanence of online content
 - The risks of AI-generated imagery and deepfakes
 - How to seek help if they are concerned
-

Social networking and personal publishing on the class Dojo app

The school will educate pupils in the safe use of social networking sites e.g. use of usernames, passwords etc.

Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Pupils/parents/carers will be advised that the use of social network spaces outside school brings a range of opportunities; however it does present dangers for pupils.

Social Networking sites

If you use Facebook, Twitter or other social networking sites you must not share anything which may bring the school into disrepute. Staff should refer to the school code of conduct regarding use of social networks. Ensure that your privacy settings are locked down and remember that these settings need to be checked every time the site owners update the site.

Managing filtering and monitoring

Currently, the school's filtering service is provided by LGFL (School Protect and Home Protect), which is an enterprise-grade filtering system accredited by the UK Safer Internet Centre.

If staff or pupils come across unsuitable on-line materials the site must be reported to the class teacher (pupils) or the Headteacher (staff) immediately.

School Leaders will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Annual Review of Filtering and Monitoring:

In accordance with KCSIE 2026, the effectiveness of the school's filtering and monitoring systems will be formally reviewed at least once every academic year, or sooner if any issues are identified.

This annual review will be conducted by:

- **The Digital Lead (SLT and DDSL)** - who is the senior leader responsible for filtering and monitoring
- **The ICT Technician** - providing technical support
- **The Designated Safeguarding Lead** - providing safeguarding expertise

The review will assess:

- Whether the filtering and monitoring systems are appropriate for the age and needs of pupils

- The effectiveness of the systems in identifying and blocking harmful content
- Any gaps or weaknesses in the current arrangements
- Whether staff are appropriately trained to use and respond to the systems
- Compliance with statutory requirements

A written record of each annual review will be maintained, including:

- Date of review
- Participants
- Findings and recommendations
- Actions taken
- Date of next review

Between annual reviews, filtering reports are checked weekly by administrators of the LGFL service for the school.

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.

Handheld technologies, including games and mobile phones, often have internet access which may not include filtering. Care will be taken with their use within the school and will be supervised.

The appropriate use of learning platforms will be discussed as the technology becomes available within the school.

Where possible, staff, students and parents will receive updates on current trends, technology or devices that pupils may come in contact with and potentially cause harm.

The school recognises the safeguarding risks associated with generative AI and will:

- Assess any generative AI tools before use in school
- Ensure filtering and monitoring requirements apply to AI tools
- Educate staff and pupils about the risks and safe use of AI
- Monitor developments in AI technology and update policies accordingly

Mobile Device guidance

Southview School has a responsibility to ensure that all data stored on its computer systems is appropriate to the needs of the organisation, is securely held and complies with the requirements of the Data Protection Act 2018, UK GDPR, and the Data (Use and Access) Act 2025. The use of portable computer devices increases the risks associated with the secure storage of data. The guidance relating to the use of school owned laptop computers and data stored on school-owned or personal removable media (e.g. flash drives/memory sticks, external hard drives) can be found in Appendix A at the back of this policy.

Pupil Use of Mobile Phones - Mobile Phone-Free Environment

Please refer to our Mobile Phone and Smart Devices policy [Mobile-phone-policy-09.26.401723291.pdf](https://www.southview-school.co.uk/09.26.401723291.pdf). A printed copy of this can be made available on request.

Staff use of personal devices

Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families in a professional capacity within or outside of the setting.

Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode and kept out of sight of children. Mobile phones or devices will not be used during teaching periods unless permission has been granted by the Head Teacher in emergency circumstances.

If members of staff have an educational reason to allow children to use mobile phones or a personal device as part of an educational activity then it will only take place when approved by the Head Teacher.

Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work provided equipment for this purpose.

If a member of staff breaches the school policy then disciplinary action will be taken as appropriate. Staff use of mobile phones during the school day should be limited.

Staff should ensure that their phones are protected with PIN codes, passwords or biometric features, in case of loss or theft.

Staff should never contact parents/carers or students from their personal mobile phone, or give their mobile phone number to students/parents/carers – except when the parent/carer is a personal friend or a family member and is known to them in a capacity other than through school. If a member of staff needs to make telephone contact with a parent/carer, a school telephone should be used.

Staff should never store parents'/pupils'/carers' telephone numbers on their mobile phone, as this allows the possibility of inappropriate contact. (See exception in previous bullet point).

Staff should never send to, or accept from anyone, texts or images that could be viewed as inappropriate.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018, UK GDPR, and the Data (Use and Access) Act 2025.

Policy Decisions authorising internet access

All staff must read and sign the Staff Behaviour Policy before using any school ICT resource.

All staff must read Part 1 of Keeping Children Safe in Education 2026 in full and sign to confirm they have read, understood and will comply with it.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

Volunteers and Regulated Activity

Following the Crime and Policing Act 2026, any person volunteering in a role that involves teaching, training, instructing or supervising children frequently (once a week or more), overnight, or more than 3 days in a 30-day period is in regulated activity.

The supervision exemption has been removed.

This means:

- Volunteers who frequently teach, train, instruct or supervise children require an enhanced DBS check with barred list information
 - The school will assess each volunteer role to determine whether it constitutes regulated activity
 - Appropriate vetting procedures will be followed before volunteers begin their role
 - Records of volunteer vetting will be maintained on the single central record
-

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor ECC can accept liability for the material accessed, or any consequences of internet access. The school will monitor 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 and concerns

Complaints/concerns of internet misuse will be dealt with by a senior member of staff.

Any complaint/concern about staff misuse must be referred to the Head Teacher (or Chair of Trustees if it relates to Head Teacher).

Complaints/concerns of a child protection nature must be dealt with in accordance with school child protection procedures. This includes:

- Children potentially viewing or discussing extremist, inappropriate or distressing materials that they have accessed online
- The making or sharing of nudes or semi-nudes (including AI-generated images)
- Online bullying or harassment
- Exposure to harmful content
- Grooming or exploitation

The school DSL and appointed deputies are responsible for acting on reports in line with (but not limited to):

- Keeping Children Safe in Education 2026
- UKCIS guidance on sharing nudes and semi-nudes
- PREVENT guidelines
- School safeguarding and child protection policies

Mental Health Concerns:

Staff should be aware that mental health problems can, in some cases, be an indicator that a

child has suffered or is at risk of suffering abuse, neglect or exploitation. Examples include:

- Self-harm
- Suicidal ideation and risk of suicide
- Eating disorders
- Anxiety and depression related to online experiences

If staff have a mental health concern about a child that is also a safeguarding concern, they should:

- Report it immediately to the DSL or a deputy DSL
- Follow the school's child protection procedures
- If a child is in immediate danger or at risk of harm, call 999

Pupils and parents will be informed of the complaints procedure.

Community use of the internet

All use of the school internet connection by community and other organisations shall be in accordance with the school E-safety policy.

Communications Policy - Introducing the E-safety policy to pupils

Appropriate elements of the E-safety policy will be shared with pupils. Pupils will be informed that network and internet use will be monitored.

Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils.

This should be addressed each year as students become more mature and the nature of newer risks can be identified.

Staff and the E-safety policy

All staff will be given access to the School E-safety Policy and its importance explained.

All staff will sign to acknowledge that they have read and understood the E-safety policy and agree to work within the agreed guidelines as part of their induction process and updated annually.

All staff must read Part 1 of Keeping Children Safe in Education 2026 in full as part of their induction and annually thereafter, and sign to confirm they have done so.

Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

Parents' and carers' attention will be drawn to the School E-safety Policy in newsletters and on the school website.

Parents should be offered E-safety training regularly with a focus on education and having an overview of tools to allow them to take control whilst not undermining trust. Parents should be encouraged to monitor device usage and question the appropriateness of the material that children access.

Parents will be informed about:

- The school's mobile phone-free environment policy and the rationale behind it
- The risks associated with the making or sharing of nudes or semi-nudes, including AI-generated images
- How to support their child's online safety at home
- The importance of age-appropriate use of social media and online platforms

Often children do not wish to be constantly online but often lack sufficient alternatives for play, travel, interaction and exploration. Parents should be encouraged, where possible to interact with their children on the internet as well as provide other opportunities for learning and recreation.

Appendix A Laptop and Removable Storage Advice

For the purpose of this policy the term "laptop" is used to describe any portable computer device including laptops, notebooks, tablet PCs, cameras, flash drives, on which school data may be stored. Your laptop is a valuable asset and an essential business tool. It needs to be protected, as does the information it stores. Remember that the laptop and the information that it contains could be valuable to thieves. By following the simple security measures listed below, you can help protect yourself and your laptop.

Teacher/Staff Responsibilities

Teachers/members of staff must take personal responsibility for the security of the equipment, software and data in their care and abide by the following:

- Laptops in cars must be stored out of sight (e.g. in covered boot). Laptops should never be left in a vehicle for prolonged periods of time or overnight.
- Always lock your laptop away when it is not in use in school.
- Un-authorized or unlicensed software must not be loaded on to the laptop.
- Ensure the laptop is not used by un-authorized persons.
- Take all reasonable steps to ensure that the laptop is not damaged through misuse.
- When travelling, laptops should not be left unattended in public places.
- Remain particularly vigilant when using your laptop and try to refrain from using it in public places (e.g. library, railway station).
- Return the laptop to school for regular health checks or when requested and ensure that the laptop antivirus software is updated by the school ICT technician (automatic updates to be reviewed by the Technician at least annually).
- Ensuring that the protection settings are left as set up by the technician (e.g. that Windows Firewall always runs, passwords are in place).
- Passwords should be kept safe. Update your passwords regularly and don't let others use them.
- Return the laptop before leaving the employment of the school.
- Report any possible security breaches (e.g. laptop stolen or misplaced) to the Head Teacher immediately.
- Ensure that the ICT Technician has noted any serial numbers for the equipment and asset tags have been created, where necessary.
- Back up your files regularly and store them securely.
- Do not allow family or friends to use your laptop, as there is a risk that school information could be compromised.
- Wherever possible, when storing data for work purposes, store the data on the encrypted drive supplied by the school.
- If you are attacked, don't risk your own safety. Hand over the laptop. It can be replaced but you can't.