

E-Safety Policy

Signhills Academy



Approved by:

Date: Spring 2026

Next review due by: Spring 2027



E-Safety Policy

Context

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Not all devices used by pupils at home will be covered by network protection as they are within the academy, and therefore an emphasis of this policy must be on understanding risks and acting accordingly.

Aims / Objectives

Teaching, learning, personal development and well-being should be enhanced through:

- the creation of a safe ICT learning environment through which pupils can develop their skills and knowledge,
- supporting everyone in being responsible users of ICT, aware of their rights and responsibilities,
- equipping users with the skills and knowledge to stay safe while using the internet and other communications technologies for educational, personal and recreational use,
- ensuring academy ICT systems are protected from accidental or deliberate misuse that could put the security of the systems and users at risk,
- ensuring that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of pupils with regard to their on-line behaviour.

Learning

A planned e-safety curriculum will ensure that pupils are:

- taught what Internet use is acceptable and what is not and given clear objectives for internet use.
- educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- shown how to publish and present information, safely, to a wider audience.
- taught to acknowledge the source of information used and to respect copyright, when using the internet.
- taught the importance of e-safe methods of searching the internet and the importance of cross-checking information before accepting its accuracy.
- taught how to report unpleasant, inappropriate and/or illegal internet content e.g. using the CEOP Report Abuse icon or Hector Protector.
- taught e-safety strategies based around the 'SMART' rules.
- taught about the safe use of social networking sites.
- taught never to give out personal details of any kind which may identify them, their friends or their location.
- taught the reasons why personal photos/videos should not be posted on any social network space without considering how the photo/video could be used now or in the future.
- taught about security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Pupils should only invite known friends and deny access to others.

Managing equipment, system security, monitoring and filtering

Sophos antivirus system is used to protect Windows-based academy machines.

Devices, such as laptops – which are used both on and off site must be regularly connected to the academy network to update.

Smoothwall is used to filter all internet access through the academy's network. Smoothwall work with the Internet Watch Foundation databases to support a safe network.

The academy receives weekly notifications from Smoothwall any potentially inappropriate searches.

Any potentially inappropriate material accessed through the academy's network by pupils or staff, must be reported to the Headteacher. A decision will then be made by the Headteacher as to whether to block the content.

Any request to have a site unblocked, should be made to the Headteacher via Smoothwall.

The academy will work in partnership with its ICT providers to ensure that systems to protect pupils are reviewed and improved, at least annually.

The academy will work in partnership with its ICT provider to ensure that filtering methods actively employ the Internet Watch Foundation CAIC list.

Physical access to servers, switches and wireless systems are restricted.

An annual audit will be used to ensure that software licences are accurate and sufficient.

Publishing content

Staff or pupil personal contact information will not be published. The contact details given online should be those of the academy.

The Headteacher will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Photographs and videos that include pupils will be selected carefully so that images of individual pupils cannot be misused.

Pupils' full names will not be used anywhere on an academy website or other on-line presence, particularly in association with photographs and/or videos.

Written permission, using the approved permission form, from parents or carers will be obtained before photographs/videos of pupils are published on the academy website or other on-line presence.

Managing emerging technologies

Emerging technologies will be examined for their educational benefit and potential risks, before use in the academy is allowed.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Signhills Academy recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Signhills Academy will refer to the behaviour policy to treat any cases where AI has been used to bully others.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the Academy.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and in line with the academy's Data Protection Policy.

Staff, Governors and Visitors

All staff, governors and visitors must read and sign the appropriate 'Code of Conduct for ICT' before using any academy ICT resource.

The academy will maintain a current record of all staff, governors, visitors and pupils who are granted access to academy ICT systems.

All staff, governors and visitors will be given access to the e-safety policy.

Users are informed that network and Internet traffic can be monitored and traced to the individual user.

Senior staff will ensure access to training, information and support is available for all staff and governors as appropriate.

All staff, governors and visitors have a responsibility to seek clarification or training, where they identify areas of e-safety as a training need.

All staff will be provided with regular e-safety information through the e-safety advisor newsletter.

Pupils

SMART rules are displayed prominently around the academy.

Pupils are informed that network and Internet use can be monitored.

The e-safety curriculum, alongside the PSHE curriculum supports pupils in developing safe and appropriate online behaviours.

Links to national events such as: Anti-bullying Week and Safer Internet Day are used to support learning.

Parents/carers and the wider family

The e-Safety Policy and advice/support on e-safety matters will be shared via the academy website, the academy brochure, information sessions and in relevant newsletters.

Parents/carers will be informed that whilst the academy will take all reasonable precautions to prevent access to inappropriate material, 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 device connected to the academy network.

Links to national events such as: Anti-bullying Week and Safer Internet Day are used to raise the profile of e-safety. This includes parents/carers being invited in to a workshop providing information about how to support their child in their online world.

Parental media expectations

For any academy event, the following information will be given to parents via invitation, posters at events and introduction as appropriate:

If you would like to take photographs and/or videos of this event, please ensure that no images/videos are shared on the Internet e.g. via social media, without consent from the parents of all children in the image/video. This is to ensure that all children, particularly those in vulnerable circumstances, are protected.

Identifying, reporting and responding to inappropriate use

The receipt of any communication that makes a person feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature, must be immediately reported to a member of staff. The recipient must not respond to any such communication.

Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official academy systems. Personal email addresses, text messaging or social media must not be used for these communications.

Following any concern raised, a CPOM must be completed as soon as practically possible and the Headteacher notified.

Review

Policy review will be led by:

Governor Team	Safeguarding
Staff Team	Senior Leadership Team
Term / Year	Spring 2026

Signed

Date

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the academy's e-safety policy for further information and clarification.

- I understand that it is a criminal offence to knowingly use an academy ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for academy business.
- I understand that academy information systems may not be used for private purposes without specific permission from the headteacher.
- I understand that my use of academy information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in the academy, taken off the academy premises or accessed remotely.
- I will report any incidents of concern regarding children's safety to the e-Safety Coordinator, the Designated Child Protection Coordinator or Headteacher.
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote and model e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will only store personal/sensitive data on the academy server or approved web-based systems; in line with the academy's Data Protection policy.
- I will actively seek e-safety training or support, in response to an identified need.
- I will ensure that my online presence does not bring the academy into disrepute.

The academy may exercise its right to monitor the use of the academy's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the academy's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Name _____ Signed _____ Date _____

Key Stage 2 E-Safety Rules

Be smart ^{on the} internet



Childnet
International
www.childnet.com

S

SAFE

Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.



M

MEETING

Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.



A

ACCEPTING

Accepting emails, text messages or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!



R

RELIABLE

Information you find on the internet may not be true, or someone online may be lying about who they are.



T

TELL

Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

THINK
UK
KNOW



www.kidsmart.org.uk

KidSMART

Visit Childnet's KidSMART website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by joining Koolaid with people all around the world.



Illustration by: [illegible]