The NEST
alternative
provision
www.thenest-ed.uk

e-safety Policy

Date written:	August 2025
Written by:	Joy Iliff
Date reviewed:	n/a 2025
Reviewed by:	n/a 2025
Approved on:	October 2025
Review date:	August 2026
Substantive changes since last review:	-

Contents

Policy aims

The NEST aims to ensure that every learner is safe on and offline. IT and online communications provide unrivalled opportunities for learning but also pose more significant and subtle risks to learners. To prepare learners for the digital world, we teach online safety (including privacy, identity theft, cyber bullying, harassment, grooming, cyber stalking, abuse and radicalisation).

Technological literacy is essential to success in the adult world. Ever developing technologies can enhance communication, information sharing, learning, socialising and leisure. We expect learners to use the following technologies in and outside of the NEST:

- Websites/blogs
- Emails/instant messaging/texts/chat rooms
- Social networking sites and services
- Artificial Intelligence (AI)
- Music/video/podcast access/downloads
- Online gaming and console gaming
- Video calls
- Smartphones/tablets/laptops

We wish to protect the interests and safety of the entire NEST community. Despite the advantages of using technologies within education, there are several inherent risks that are not currently controlled except at user level. All IT users must be aware of the range of risks associated with IT use.

We aim to teach our learners to be safe and legal online through developing appropriate behaviours and critical thinking skills.

Links to legislation and guidance

This policy has been written in compliance with the following legislation and guidance:

- Data Protection Act 2018
- Sharing Nudes and semi-nudes: advice for education settings working with children and young people – responding to incidents and safeguarding children and young people 2020
- The Prevent duty: safeguarding learners vulnerable to radicalisation 2023
- Teaching online safety in schools 2023
- Online Safety Act 2023
- Working together to safeguard children 2025
- Keeping children safe in education 2025

Associated policies and further reading

This policy should be read in conjunction with the following associated policies and documents:

- Anti-Bullying Policy
- Behaviour Policy
- Community Contract
- Community Contract - Staff
- Data Protection Policy
- Health & Safety Policy
- Safeguarding & Child Protection Policy

Definitions

Device – phone, tablet, laptop or computer that can access the internet.

e-safety – protection of digital technology/system users against harm from:

- Content – illegal, inappropriate, or harmful content (e.g. violence, discrimination, pornography, fake news, self-harm & suicide, radicalisation, extremism)
- Contact – harmful online interaction (e.g. peer pressure, grooming or exploitation for sexual, criminal, financial, radicalisation purposes)
- Conduct – online behaviour increasing harm (e.g. sharing violent media, cyber-bullying, making, sending, receiving explicit images – nudes, semi-nudes, pornography)
- Commerce – gambling, unsafe advertising, phishing, financial scams.

Software – programs or applications downloaded or installed on devices.

Roles and Responsibilities

Directors

Directors are responsible for the overall safety of the NEST community (including online). It is their responsibility to:

- Approve and review this policy and related documents and procedures
- Facilitate staff training on e-safety and relevant policies and procedures
- Invest in safe equipment and services
- Ensure fair administration of this policy
- Ensure secure and encrypted data storage
- Oversee investigations in e-safety breaches

See Community Contract – staff, Behaviour Policy, Whistleblowing Policy for more information.

Designated Safeguarding Lead

The DSL is responsible for everyday e-safety issues. It is their responsibility to:

- Ensure adherence this policy by all members of the NEST community
- Keep up to date with emerging e-safety threats and strategies
- Devise and arrange teaching programmes for e-safety
- Deal with issues arising from e-safety breaches
- Ensure NEST devices have appropriate filters, protections and limits
- Contact caregivers if a concern is raised about a learner

Staff

Embedding and role modelling safe internet usage while monitoring as possible learner internet usage. It is their responsibility to:

- Discuss opportunistically and through scheduled discussions (flock huddles) the positive and responsible use of technology and social media
- Sign Acceptable Use Agreement – before using NEST devices
- Foster a culture of talking and listening
- Model responsible technology use
- Monitor learner screen time during sessions
- Prevent unsupervised use of NEST devices
- Train as required to and remain up-to-date with e-safety issues
- Report concerns to DSL
- Apply RAP regarding the use of technology

See Behaviour Policy for RAP and Child Protection & Safeguarding Policy.

Learners

Learners have responsibility for their own online behaviour and safety at an appropriate level for their capacity. It is their responsibility to:

- Tell staff if they observe incorrect technology use in the NEST community
- Develop a critical lens for online content and learn about e-safety issues
- Sign Acceptable Use Agreement part of Community Contract

See Behaviour Policy for more on RAP.

Caregivers

Caregivers are vital in the maintenance of learners' e-safety. It is their responsibility to:

- Engage in consultation and discussion with the NEST about e-safety
- Share concerns about their learner's e-safety with the NEST
- Promote learner e-safety outside of the learning environment.

Community voice

We value lived experience at the NEST, and we believe that centring the voice of lived experience is a route to better care. The insight of learners, caregivers, staff and collaborators are invaluable in shaping an environment of trust, collaboration and co-ownership. Intentionally prioritising the perspective of learners and caregivers supports educator understanding of learner needs and can empower learners to contribute to meaningful decision making and to take an active role in their learning. Valuing staff and collaborator feedback can facilitate closer co-working and productive communication.

We understand the particular importance of involving students in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas. Part of the development of the Community Contract will involve thinking directly about e-safety and use of technology. We also encourage caregivers to give us their opinions and worries relating to e-safety.

Processes

Education

Learners must be given e-safety guidance on a meaningful and regular basis. We seek new opportunities to embed and promote e-safety and frequently monitor learner understanding and awareness through structured sessions and opportunistic learning.

Induction

Induction includes assessing awareness of e-safety issues and practices. During induction they read and sign a Community Contract including e-safety practice.

Curriculum

In flock huddles (see Behaviour Policy), learners receive capacity-appropriate, short sessions on:

- Privacy
- Identity theft
- Cyberbullying (see Anti-Bullying Policy for reporting and support)
- Online harassment and abuse
- Grooming, cyberstalking and sexual exploitation
- Radicalisation
- Legislation relevant to data protection and intellectual property
- Respecting other people's information and images
- Appropriate and safe online conduct
- Digital footprint (including images)

Embedded throughout these sessions will be the duty to report, reporting routes (see Safeguarding & Child Protection Policy) and how to access support according to needs. Each mini session will be followed by a short quiz to assess learning. See Appendix B for outline of how this might be delivered.

When possible and appropriate, we will offer EL3 Essential Digital Skills Qualification which tests many e-safety skills among wider computer literacy.

Opportunistic and passive learning

Through taking a proactive, opportunistic approach to topical e-safety issues, staff can model best practice using digital technologies and online platforms as well as facilitate conversations according to the Community Contract. A strong focus is placed on critical thinking and self-reflection in all aspects of the NEST which can be applied to e-safety practices. In all projects, that e-safety is relevant to, staff will prompt learners to consider how what they have already learnt can be applied in this context to support consolidating learner.

Use of devices and systems

For the end-of-day review, learners may use their own devices (a RAP system privilege) or a NEST device if not. Opportunistic research via search engine may also happen throughout the day. Where possible Staff should keep these on NEST devices, but we recognise the value of learners acquiring search skills.

Own devices

Any member of the NEST community using their own device on-site or on a trip must complete an Acceptable Use Agreement (Appendix). This contains several recommendations for usage of device including:

- Device must be locked with a PIN, password or biometric security. When device is left unsupervised, it must be locked.
- Anti-virus protection for all devices is strongly recommended
- Filters and controls are recommended. For learners, caregivers to put in place controls. For staff, if a learner may at any point have their device, controls and filters should be applied temporarily while they are at work.
- Caution around downloading and installing programmes or applications
- Staff devices are encrypted if data or passwords are saved on them

Necessary personal device usage

For personal or medical needs, a staff member or learner may need to have consistent access to their device. This must be communicated to staff/Directors who will support that individual in their need to have their device.

Device search and deletion

If staff observe graphically violent or pornographic media or that which is relevant to a crime on a learner's device it should be immediately reported to DSL who will advise on next steps. These images can be deleted by staff unless it is necessary for internal investigations or to pass it onto the police. Staff must be aware of local regulations and guidelines around "good reason" to examine or erase data or files. Where possible the learner will be asked to delete it to minimise staff contact with learner media and devices.

Misuse

Where devices or systems are used for criminal activities or those inappropriate to an educational setting, a report will be logged with the DSL.

Misuse includes: cyberbullying, sexting (sharing youth produced sexual images), involvement in radicalisation, grooming, bullying, harassment or abuse.

NEST devices and systems

- All NEST devices are protected according to the above recommendations.
- All logins for NEST email and training must use a "strong" password (at least 8 characters, upper and lower case letters, numbers, special character). Login credentials are stored securely.
- Administrator permissions are enabled on all NEST devices so only Directors can load software.
- Any software downloaded or installed must be properly licenced and free of viruses.
- Any loss or unauthorised use of a NEST device reported to Directors immediately.

Backup and disaster recovery

The backup regime in case of data loss includes:

- Secure encrypted, daily, online backup
- No data is stored solely locally
- Testing (renaming and retrieving sample files) every 6 months

This will be conducted as rapidly as is feasible, prioritising critical information and systems in retrieval.

Social media and communication practices

Calls to any stakeholders should be directed through our proxy number and staff should not accept contact on their personal phone numbers.

Social media

For most social media platforms, users must be over 13 years old, but we acknowledge many will have access to platforms before this age. Staff and learners can never be in a shared social network. Staff and caregivers should not be in shared social networks unless the relationship pre-dates the young person becoming a learner at the NEST, in which case a Declared Relationship form is completed (Appendix C). Learners can add @thenest-ed on Instagram.

Responsible posting

Staff and learners are made aware of the impact of what they post and aware of professional/responsible boundaries (see above). The NEST community are all made aware they must not knowingly or recklessly:

- place a young person (learner or not) at risk of or cause actual harm
- bring the NEST into disrepute
- breach confidentiality
- breach copyright
- breach data protection legislation
- do anything that could be considered discriminatory against, or bullying or harassment of, any individual

Learners taught to refrain from posting inappropriate (e.g. violent or sexual), offensive or embarrassing (even to themselves) content. This includes:

- making offensive or derogatory comments relating to sex, age, gender identity, race (including nationality), disability, sexuality, religion or belief
- bullying another individual
- posting links to or endorsing discriminatory or offensive material

Staff and learners who discover an unsuitable post has been shared or posted by staff or learners tell DSL.

Educational purposes

For young people social media is often stated as a primary place of learning and harnessing this for productive ends is central to our ethos. Learners will prepare anonymous posts for the NEST Instagram account under supervision and with comments disabled for protection against online harassment. No learner or staff member's face will be shown on posts. All posts are vetted by a member of staff before posting and any with concerns of inappropriate content are not posted.

Vetted, informational or creative posts may be used to spark conversation or inspire creative work or debate but at no point will a learner be allowed to scroll without a specific aim. Staff must not be observed using social media except for educational or modelling purposes.

emails

Staff who need to communicate on behalf of the NEST have email addresses for this purpose and should not use personal email accounts to contact caregivers, commissioners, other providers or external agencies. Digital communication between staff and caregivers must be professional in tone and content. All contact for the learner (i.e. educational content) is sent via learner NEST email. All staff are made aware of the risks of fraudulent emails, spam and phishing to work accounts. Staff will never respond to these, block senders/mark as spam and log this in spam, phishing, fraudulent emails tracker (Appendix D). Phishing will also be reported to the Anti-Phishing Working Group.

Appropriate content

The NEST uses websites, applications and programmes appropriate to the development stages of the learners involved.

Content controls

To meet our duty to safeguard learners (including Prevent) the DSL:

- Manages filtering and monitoring systems for controlling content access
- Reviews filtering and monitoring systems (against safeguarding needs)
- Blocks harmful and inappropriate content without unreasonably impacting education

Inappropriate content

If inappropriate content is found (e.g. violent, discriminatory, pornographic or horrific) the user should:

- Turn off the monitor or minimise the window.
- Report the incident to staff or DSL

The person receiving the report should ensure the wellbeing of the person who witnessed the content and then collect information (particularly url) without the witness being re-exposed to report to DSL (see below).

Media for learning

The taking and sharing of images poses a significant safeguarding risk to the subject of the photos. Learners and staff are encouraged to think of images as being permanent and to consider the potential long-term impacts. Learners must not share, publish or distribute images of others (staff or learners).

Recordings and images may be used for educational purposes. When this is necessary, learners are made aware of recording and are able to review and delete any media they do not want to be kept. Where possible a NEST device is used. Where they must be taken on a personal one, they are transferred to encrypted storage as soon as possible and deleted locally. Learners may record their own work and share via Canva for assessment.

When using other digital media (i.e. that found online) staff must ensure that these do not breach copyright and are necessary, relevant and appropriate.

Social media for promotion

Caregivers are asked for consent to share images and recordings of their learner on the website or social media at admission. Social media are carefully selected to comply with best practice. Recordings and images are not published online without additional consultation with the learner.

Caregiver support

The NEST community must work closely together to promote e-safety for all. Not all caregivers feel equipped to protect their child online. We offer support, signposting and sessions for caregivers who wish guidance on enabling "parental" controls, monitoring/controlling the learner's internet usage, concerns about online safety and content. Open communication around e-safety is encouraged through email,

social media posts and in face-to-face meetings. Caregivers are told when their learner is involved in an incident or shows concerning online behaviours.

Concerns

For raising concerns more generally (including e-safety) see Safeguarding & Child Protection, Anti-bullying and Behaviour Policies

Raising concerns

All members of the NEST community have a duty to report as soon as reasonably possible to the DSL any:

- Communication that is uncomfortable, sexually explicit, offensive, discriminatory, threatening or bullying
- Accidental access to inappropriate (violent or sexual) content at the NEST
- Misuse of any digital services or devices while at the NEST
- Storage/sharing/sending of abusive or inappropriate messages or content via personal devices
- Online material believed to be illegal

DSL investigation

The DSL will then:

- Log incident in safeguarding log
- Investigate

- Take appropriate action (consultation if necessary) which could include:
    - Report the incident to caregivers
    - Report to LADO, police or other external agencies as necessary
    - Report illegal online content (IWF or Child Exploitation and Online Protection - CEOP)
    - Meet with caregivers, commissioners, LADO or other child protection staff as necessary
    - Put sanctions in place
    - Treat deliberate attempts or incidences of viewing inappropriate content as a behaviour concern and record in Behaviour log

Outcomes

Primary response to all instances is led by compassion and a desire to educate.

Learners

The 4Es of the RSUCS behaviour process focus on understanding potentially harmful behaviours and speech to be able to educate. If at evaluation, no changes of behaviour have been found the learner may lose access to devices and systems. Under the RAP system, learners showing inappropriate e-safety behaviours may lose access to use devices or systems. We may engage support from external agencies to deal with serious e-safety behaviour incidents.

Staff

Staff are bound by the Community Contract - staff. Intentional or persistent non-compliance addressed as a disciplinary matter.

Record keeping and information sharing

Learner educational media and records

All self-reports, digital media, documents and data will be stored on the NEST OneDrive. Where possible, all files shared digitally via OneDrive. If digital storage devices (USB, portable drive) needed for example for transferring work to home computer without internet, it must be provided by the NEST and cleared and formatted before use.

Record of e-safety incidents

A Safeguarding Concerns Form (see Safeguarding & Child Protection Policy) will be completed for all e-safety safeguarding concerns, regardless of outcome. This will then be managed as any other safeguarding concern record (see Data Protection Policy). An e-safety concern should include any urls involved and information about users or devices as relevant.

Training

Staff training, learning and development are highly encouraged and facilitated by the NEST. All staff are expected to complete minimum training requirements as outlined in our Staff Training Plan and additional learning and related continued professional development are strongly supported.

All staff receive induction training delivered both internally and externally. Induction training includes the following e-safety elements:

- KCSIE 2025 Document reading & Quiz
- Safeguarding & Child Protection (Sept 2025 version)

The DSL and DDSL will also complete additional training pertinent to the role:

- Designated Safeguarding Lead training
- E-safety training

All staff training is logged and stored in our staff records. Refresher courses are facilitated according to best practice. Additional learning sessions may be run at the DSL throughout the year as emerging issues or strategies are identified.

Review

This policy will be reviewed annually at a minimum. Updated policies will be made available locally and on our website (www.thenest-ed.uk). Ad hoc amendments will be made as new information becomes available and to align with any legislative changes as they arise. Stakeholder feedback, particularly that of learners and caregivers, will be invited and incorporated as much as is practicable. Where quantitative data are available these will be analysed and embedded in policies updates.

Initial assessments of e-safety and responses to learning questions (Appendix B) will be analysed to ascertain if teaching is effective. The phishing, spam and fraudulent email log will be analysed to identify potential security risks. Anonymised e-safety concern information will be used for identifying trends. Surveys of caregiver and learner understanding of e-safety will be periodically conducted and used to review, safety measures, policy and curriculum.

Appendices

Appendix A – Acceptable Use Agreement – Learner-friendly

Appendix B – Example of Flock Huddle learning activities

Topic	Potential sub-topics and learning activities	Learning check questions
Privacy	Algorithms video - BBC or Algorithms TED talk – followed by a discussion	Why do social media services want to "perfect" your algorithm? What information do they use to do this?
	Cookies – activity using string and stickers Discussion about why we have opt out now.	What do cookies do? Why would you want to disable them?
	Data scraping – market activity where you have to buy if advertised the correct product.	How can a company find out things about you from your online activity? What happens to collected data?

Appendix C – Declared Relationship agreement

Appendix D – Spam, phishing, fraudulent email tracker