HAIR ACADEMY

E-Safety Policy

Approved by: Harvey Schofield

Last reviewed on: 03/2026

Next review due: 03/2027

Introduction:

New You Hair Academy acknowledges the vital role of creating a secure online environment for both students and staff. Our commitment to E-Safety is articulated in this policy, emphasising the protection of students from online risks, responsible internet usage, and the cultivation of digital citizenship. By adhering to this policy, our goal is to enable students to make informed decisions while engaging with digital technologies.

Statutory Framework:

This policy operates in accordance with:

- Keeping Children Safe in Education (2025)
- The DfE Filtering and Monitoring Standards (2023)
- Working Together to Safeguard Children (2023)
- The Education Act 2002 (Section 175)
- UK GDPR and Data Protection Act 2018

Online safety is recognised as a safeguarding matter and forms part of the academy's wider Safeguarding & Child Protection Policy.

Responsibility:

The Strategic Lead has overall responsibility for online safety.
The Designated Safeguarding Lead (DSL) has operational responsibility for responding to online safety concerns and ensuring appropriate safeguarding action is taken.

All staff are responsible for identifying and reporting online safety concerns.

User Responsibility:

Students and staff bear the responsibility for their conduct when utilising digital technologies on provision premises or during provision-related activities. Compliance with the provision's Acceptable Use Policy (AUP) regarding responsible technology use is mandatory. Users are encouraged to promptly report any E-Safety concerns or incidents to a staff member.

Education and Awareness:

New You Hair Academy will deliver age-appropriate E-Safety education to all students. Regular E-Safety awareness sessions for staff, parents, and students aim to keep them well-informed about online risks and best practices. The curriculum will cover responsible online behaviour, digital footprints, cyberbullying, privacy settings, and the significance of respecting others' online rights and well-being.

Introducing the E-Safety Policy to Pupils:

- E-Safety rules/advice will be displayed in all networked rooms and classrooms using mobile laptop computers.
- Pupils will be informed about the monitoring of network and internet use.
- Sanctions for violating E-Safety rules within provision premises will be available for parents to review.
- Pupils are required to sign the Pupil Acceptable Use Agreement before gaining access to New You Hair Academy systems and must adhere to it consistently.
- Awareness of plagiarism, copyright regulations, reporting abuse or misuse, and understanding New You Hair Academy policies on mobile phones and digital devices is essential.
- Pupils should also comprehend New You Hair Academy's policies on image use and cyberbullying, along with adopting good E-Safety practices beyond provision premises.

Staff and the E-Safety Policy:

- All staff members will receive the New You Hair Academy E-Safety Policy, with its importance explained.
- New staff will be provided with the New You Hair Academy E-Safety Policy during their induction.
- Staff should be aware of the potential monitoring of internet traffic.
- Discretion and professional conduct are emphasised.
- Staff overseeing filtering systems or monitoring ICT use will be supervised by senior management, following clear procedures for issue reporting.
- Reminders for both pupils and staff to log off workstations are in place.
- Downloading and installing executable files from the internet (or elsewhere) without permission is prohibited, with unauthorised files logged.
- Pupils using proxy sites to access banned websites will meet with the Director of Alternative Education, who will follow up with New You Hair Academy's sanction policy when necessary.
- Serious abuse cases may involve sending a letter home, specifying the content of the website, and adding it to the filtered list. Staff should integrate E-Safety teaching within the curriculum when electronic devices are used.
- Staff should refer to the following websites for guidance and further information:

  https://www.ceop.police.uk/
  https://www.thinkuknow.co.uk
  https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

Filtering and Monitoring:

Filtering and monitoring systems are reviewed regularly by senior leadership to ensure they are effective and appropriate to the age and risk profile of students.

Monitoring systems are designed to identify safeguarding risks, including but not limited to:

- Child sexual exploitation
- Radicalisation
- Self-harm content
- Bullying and harassment
- Access to inappropriate material

Concerns identified through monitoring will be referred to the DSL without delay.

The effectiveness of filtering and monitoring systems forms part of the academy's safeguarding review processes.

Online Safeguarding Risks:

The academy recognises that students in alternative provision may be at increased vulnerability to online exploitation and therefore adopts a proactive and vigilant approach to digital safeguarding.

The academy recognises that online safety risks may include:

- Cyberbullying
- Online grooming
- Sexual exploitation
- Youth produced sexual imagery
- Radicalisation and exposure to extremist material
- Online fraud and exploitation
- Self-harm and suicide-related content
- Misuse of artificial intelligence tools

Any such concerns will be treated as safeguarding matters and handled in line with the Safeguarding Policy.

Mobile Phones and Personal Devices:

New You Hair Academy recognises that mobile phones and personal devices present both opportunities and safeguarding risks.

The use of mobile phones during the academy day is governed by the Behaviour Policy and Mobile Phone Expectations. Students may not use personal devices during lessons unless explicitly authorised by staff for educational purposes.

The following are strictly prohibited:

- Accessing inappropriate or harmful content
- Recording staff or students without consent
- Sharing images or videos without consent
- Engaging in cyberbullying or harassment
- Circumventing filtering systems through VPNs or proxy sites
- Using artificial intelligence tools to create harmful, explicit or deceptive content

Where misuse involves safeguarding concerns (e.g. sexual imagery, exploitation, grooming, extremist content), the matter will be immediately referred to the Designated Safeguarding Lead and recorded on CPOMS.

The academy reserves the right to search, confiscate and examine mobile devices in line with DfE Searching and Confiscation guidance where there are reasonable grounds to suspect misuse.

Reporting and Response:

All online safety concerns must be reported to the Designated Safeguarding Lead. Concerns will be recorded on CPOMS and managed in accordance with safeguarding procedures.

Where appropriate, external agencies including Children's Social Care or Police will be informed.

Reported incidents will be addressed promptly and appropriately, following the provision's behaviour and safeguarding policies.

The provision will maintain records of reported incidents and actions taken, ensuring confidentiality and compliance with data protection regulations.

Partnerships and Collaboration:

New You Hair Academy will collaborate with parents, external agencies, and community partners to enhance E-Safety practices and support students' well-being in the digital world.

The provision will actively engage in E-Safety initiatives, staying up-to-date with emerging risks and adopting relevant measures to mitigate those risks.

Review and Evaluation:

This E-Safety Policy will be reviewed annually to ensure it remains effective and aligned with changing technologies, legislation, and best practices.

Feedback from staff, parents, and students will be considered to improve the implementation of E-Safety measures.

Glossary of Terms:

Algorithm
A system used by social media platforms to determine what content users see. Algorithms may expose young people to harmful, extremist or exploitative content.

Artificial Intelligence (AI)

Computer systems capable of performing tasks that normally require human intelligence. AI tools can generate text, images, or videos and may be misused to create harmful or explicit content.

Blog
A blog, also known as a weblog, is a form of online diary or journal. Blogs contain short, frequently updated posts, arranged chronologically with the most recently posted item appearing at the top of the page. In addition to text, blogs can contain photos, images, sound, archives and related links, and can incorporate comments from visitors. MoBlogging is blogging by mobile phone.

Bluetooth
Bluetooth is a telecommunications industry standard which allows mobile phones, computers and PDAs to connect using a short-range wireless connection.

Bluejacking
Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers.

Caching
The process of temporarily storing files, such as web pages, locally to enable quick access to them in the future without placing demands on network resources.

Chat room
An area on the internet or other computer network where users can communicate in real time, often about a specific topic.

Filtering
A method used to prevent or block users' access to unsuitable material on the internet.

Firewall
A network security system used to restrict external and internal traffic.

Hacking
The process of illegally breaking into someone else's computer system, breaching the computer's security.

Information and communications technologies (ICT)
The computing and communications facilities and features that, in an educational context, variously support teachers, learning and a range of activities.

Internet Service Provider (ISP)
A company providing a connection to the internet and other services, such as browser software, email, a helpline, web space and subscriber-only content.

Live Streaming
Broadcasting live video content over the internet. Live streaming can expose young people to grooming, exploitation or inappropriate contact.

Personal Digital Assistant (PDA)
A small, mobile, handheld device that provides computing and information storage/retrieval capabilities, and possibly phone facilities too.

Pharming
Pharming is similar to phishing, however pharming seeks to obtain information through domain Spoofing.

Phishing
An attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic Communication.

Sexting (Youth Produced Sexual Imagery)
The creating, sharing or forwarding of sexual images or videos of under-18s via mobile phones, apps or online platforms. This is a safeguarding matter and may constitute a criminal offence.

Spam
Unsolicited junk email. The term is also used to describe junk text messages received via mobile phones. A related term, spim (or spIM), describes receiving spam via instant messaging.

Spoofing
Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a virus-infected computer). Spoofing is typically practised to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammer.

Trojan horses
A virus which infects a computer by masquerading as a normal program. The program contains additional features added with malicious intent. Trojan horses have been known to activate webcams, for example, without the knowledge of the PC user.

Virtual Private Network (VPN)
A tool used to mask internet activity or bypass filtering systems. The use of VPNs to access blocked content on academy systems is prohibited.

Video Conferencing
The process of conducting a conference between two or more participants over a network, involving audio and often text as well as video.

Virus

A computer program which enters a computer and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard drive, including the system software. All users are advised to guard against this by installing anti-virus software.

Webcam

A webcam is a camera connected to a computer that is connected to the internet. A live picture is uploaded to a website from the camera at regular intervals, typically every few minutes. By looking at the website you can see what the camera sees – almost as it happens.