NIGHTINGALE COMMUNITY ACADEMY
ONLINE SAFETY POLICY

Written by:	Pedro Fuentes
Reviewed by:	Sarah Brooks
Date of last review:	January 2026
Date of next review:	January 2027

Introduction

At Nightingale Community Academy, the safety and welfare of our pupils is of the utmost importance. Ensuring that pupils can safely access new technology and learn how to participate in the digital world without compromising their safety and security is a key part of delivering a well-rounded programme of education.

This policy sets out our approach to online safety, whether using new technology within Nightingale Community Academy or at home, including accessing remote learning, and the safe and responsible use of artificial intelligence (AI), generative tools and automated digital services.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (herein referred to as 'mobile phones') and AI-enabled platforms and tools.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Our approach to online safety is based on addressing the four key categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism, including AI-generated or algorithmically promoted content;
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes, including AI chatbots, automated accounts and deepfake identities;

- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying, including the misuse of AI to create or alter images, video, text or audio
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams, including AI-driven scams, impersonation and automated fraud.

Statutory requirements

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, **Keeping Children Safe in Education**, and its advice for schools on:

- **Teaching Online Safety in Schools**
- **Preventing and Tackling Bullying** and **Cyber-Bullying: Advice For Headteachers and School Staff**
- **Relationships And Sex Education**
- **Searching, Screening and Confiscation**

It also refers to the DfE's guidance on **Protecting Children From Radicalisation.**

It reflects existing legislation, including but not limited to the **Education Act 1996** (as amended), the **Education and Inspections Act 2006** and the **Equality Act 2010**. In addition, it reflects the **Education Act 2011**, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement and articles of association.

Roles and responsibilities

Governors will:

- Review and approve this policy not less than annually.
- Agree and adhere to the IT Acceptable Use Policy.
- Ensure that online safety is a running and interrelated theme of Nightingale Community Academy's whole school approach to safeguarding and related policies and/or procedures, including the school's Safeguarding and Wellbeing Offer.

- Ensure that the school's approach to promoting and upholding online safety is suitably tailored to the needs and aspirations of Nightingale Community Academy pupils as well as the specific risks and opportunities they may encounter because of their needs and within their local communities, **including risks linked to AI, manipulation and online exploitation.**

The Principal will:

- Ensure that staff understand this policy, and that it is being implemented consistently throughout the school.
- Review and update this policy not less than annually.
- Monitor the impact of online safety measures as set out in this policy, through regular monitoring of safeguarding practice across the school (e.g. termly safeguarding audit, data analysis, review of Safeguarding and Wellbeing Offer, pupil voice).
- Ensure that staff have access to high-quality and relevant training on online safety matters, to enable them to effectively support pupils, including training on AI risks, online coercion and digital manipulation.

The Designated Safeguarding Lead (DSL) will:

- Take lead responsibility for online safety in school.
- Support the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Work with the Principal, ICT manager and other staff as necessary to address any online safety issues or incidents, including those involving AI, deepfakes or automated platforms.
- Manage all online safety issues and incidents in line with the Child Protection, Adult Protection & Safeguarding Policy
- Ensure that any online safety incidents are logged via CPOMS and dealt with appropriately in line with this policy.
- Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Liaise with other agencies and/or external services as necessary.
- Provide regular reports on online safety in school to the Principal.

OHCAT IT staff will:

- Put in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated regularly to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material and AI-generated harmful content.
- Ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conduct full security checks and monitoring of the school's ICT systems regularly.
- Block access to potentially dangerous sites and, where possible, prevent the downloading of potentially dangerous files and unapproved AI tools.

All staff, including contractors, agency staff, and volunteers, will:

- Maintain an understanding of this policy
- Implement this policy consistently
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet, and ensure that pupils follow the school's terms on acceptable use
- Work with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Respond appropriately to all safeguarding reports and concerns, including those relating to cyber-bullying and sexual violence/harassment (whether on- or offline), maintaining an attitude of 'it could happen here', including incidents involving AI misuse, impersonation or digital coercion

Parents/carers are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.
- Monitor the usage of school independent learning systems (Google Classroom) and support the appropriate usage of homework and revision submission

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? **UK Safer Internet Centre**
- Hot topics **Childnet International**
- Parent resource sheet **Childnet International**

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms of acceptable use.

Educating pupils about online safety

Nightingale Community Academy will support pupils' understanding of online safety across all key stages. They will be provided with lessons around topics of online safety in their PSHE lessons (see below). Across the academic year, pupils will also be provided with opportunities to explore and discuss online safety through a range of independent activities such as guest speakers, assemblies, and small group drop-down sessions.

For pupils with SEMH needs, learning will be adapted to support emotional regulation, impulse control, online decision-making and recognising when digital interactions may be harmful, manipulative or misleading.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

This will include recognising that some images, voices or messages they see or hear online may be created by computers (AI) and may not be real.

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Understand online bullying
- Identify a range of ways to report concerns about content and contact

This will include learning that people, pictures or videos online may be fake, edited or created by AI, and that this can be used to trick, scare or upset people.

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online and face-to-face relationships, including respecting others, even when anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information, including awareness of the risks associated with people they have never met
- How information and data are shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

This will include understanding that AI tools can pretend to be real people, generate messages, images or videos, and may be used to manipulate or groom children.

In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- Understand accountability and prevention of online bullying

This includes recognising deepfakes, AI-generated messages, impersonation and online manipulation.

Pupils in Key Stage 4 will be taught to:

- Understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- The law in respect of online safety, and how to report a range of concerns

This includes understanding the legal, emotional and safeguarding risks of AI-generated images, fake videos, voice cloning and online impersonation.

By the end of secondary school, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further, and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties, including jail
- How information and data are generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report or find support if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

This includes understanding that AI-generated images, videos or messages can be used to pressure, shame, blackmail, or emotionally harm others, and that sharing or creating such material is never safe or acceptable.

The safe use of social media and the internet will also be covered in other subjects where relevant.

Communication with families

The school will raise parents' awareness of internet safety in letters or other communications home, and in information on our website. This policy will also be shared with parents when pupils are inducted, and parents will acknowledge that the policy is understood. Online safety will also be covered during parents' evenings.

The school will let parents know:

- The systems that the school uses to filter and monitor online use.
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Principal.

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. As with other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. Please also refer to our Anti-Bullying Policy, Behaviour Policy and the Child Protection, Adult Protection & Safeguarding Policy.

Cyber-bullying also includes harm caused using artificial intelligence (AI), such as AI-generated abusive messages, deepfake images or videos, altered or manipulated content, voice cloning, and impersonation designed to deceive, humiliate or threaten others.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others, including becoming aware that they have participated in cyber-bullying. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including when they are a witness rather than the victim.

This includes understanding that harm can occur through AI-generated content, automated messages or digitally manipulated media.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Opportunities to discuss include during form time, within the curriculum, e.g. PSHE, during assemblies and Student Council meetings.

For pupils with SEMH needs, this will include explicit teaching about emotional impact, online manipulation, and how AI and digital tools can be used to exploit trust, impulsivity or emotional vulnerability.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the Behaviour Policy, including safeguarding and supporting pupils involved. Where illegal, inappropriate or harmful material has been spread among pupils, the school will take all necessary steps to safeguard pupils, including using all reasonable endeavours to ensure the incident is contained and liaising with police or other external agencies as appropriate. This includes incidents involving AI-generated or manipulated content, which may be treated as serious safeguarding concerns.

The use of electronic devices in school

Nightingale Community Academy has a “no electronic device” policy for pupils, to mitigate distractions in lessons and to ensure the safety of all members of the community. Phones will be collected as students enter the building each day and returned to them upon dismissal. All electronic devices will be stored and locked in a secure area. Should a pupil refuse to hand in their phone, a search may be conducted (see below). Pupils will not be permitted to enter classroom settings until electronic devices are handed in to a member of staff. 6th Form students are exempt from this device policy but subject to continual review. Where issues arise, individual students may be required to hand in their devices for an agreed period or indefinitely.

This includes devices capable of accessing AI tools, chatbots, image generators, video editors, or voice-cloning software.

Regarding pupil searches, the Principal, and any member of staff authorised to do so by the Principal, can search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, the authorised staff member will:

- Assess how urgent the search is, and consider the risk to other pupils and staff
- Explain to the pupil why they are being searched, how the search will happen, and allow them to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.
When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

This includes the use of AI tools to generate abusive, threatening, misleading or sexually harmful material.

If inappropriate material is found on the device, it is up to the staff member, in conjunction with the safeguarding leads, to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Do not view the image
- Confiscate the device and report the incident to the DSL immediately. The DSL will decide on what to do next, in line with the DfE's latest guidance on **Screening, Searching, and Confiscation** and the UK Council for Internet Safety (UKCIS) guidance on **Sharing Nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People**

This applies equally to AI-generated, altered or synthetic images and videos.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on **Screening, Searching, and Confiscation**
- UKCIS guidance on **Sharing Nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People**
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Rules for publishing material online

School websites are a valuable tool for sharing information and promoting pupils' achievements. We recognise the potential for abuse. Therefore, the following principles will always be considered:

- If an image, video or audio recording of a pupil is used, their surname should not be used
- Staff must not take photographs of pupils using their personal devices
- Files should be appropriately named
- Only suitable images should be used
- Parents/carers can withdraw permission
- Copyright must be respected
- Content should be polite and respectful
- Material must be checked by SLT before publishing
- Staff must not post images of pupils or families on personal social media
- Staff must obtain permission before posting images of staff

Children will only use first names or avatars.

When photos and videos are permitted at events, parents must not publish them online.

The creation or sharing of AI-generated or AI-edited images, video or audio of pupils or staff (including deepfakes or voice clones) is strictly prohibited without written consent and safeguarding approval.

Training

All new staff members receive training on safe internet use, cyber-bullying and online radicalisation.

All staff receive refresher training annually. Updates include safeguarding and modern technologies.

By way of this training, all staff are made aware that:

- Technology is a major safeguarding risk
- Children can abuse peers online
- Online elements may be part of physical or sexual abuse
- Children with SEND are especially vulnerable

This includes understanding how AI, algorithms, chatbots and digital manipulation can be used to groom, deceive or exploit SEMH pupils.

DSLs receive Level 3 training. Governors and volunteers receive appropriate training.

Guidance on the use of social media

Staff may use social media professionally but must not discuss pupils or colleagues. Staff must not accept pupils as contacts or share personal details.

Staff must not use AI tools to generate messages, images or content that represent, refer to or simulate pupils, families or colleagues.

Monitoring arrangements

This policy will be reviewed and approved annually by the Principal and the Local Governing Body and updated in response to emerging technologies, including artificial intelligence.

Related policies and documentation

- Anti-Bullying Policy
- Anti-Radicalisation Policy
- Behaviour Policy
- Child Protection, Adult Protection and Safeguarding Policy and Procedures
- Data Protection Policy and related documentation
- Dignity at Work Policy
- IT Acceptable Use Policy
- Safeguarding & Wellbeing Offer
- Social Media Policy
- Staff Code of Conduct
- Student Mental Wealth, Health and Wellbeing Policy