Online Safety Policy (including use of social media, mobile, smart technology and AI)

Date Reviewed: January 2026

Next Review: January 2027 or after significant government policy change

Reviewed By: Sarah Logan

Policy Aims

This online safety policy lays out our approach to the use of the internet, including social media, mobile phones, smart technology and AI within the Next Steps Education community (students and parents/carers, our team, tutors and mentors).

It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2025 and 'Working Together to Safeguard Children' 2018.

The purpose of this policy is to:

- Safeguard and protect all members the Next Steps Education community online
- Identify approaches to educate and raise awareness of online safety throughout our community
- Enable all our team to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns.

Next Steps Education accepts that online safety covers a considerable and ever-changing range of issues which can be broadly categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate, or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm
- Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Policy Scope

Online safety is an essential part of safeguarding. Next Steps Education acknowledges our duty to ensure that all students and our team are protected from potential harm online. The internet and associated devices, such as computers, tablets, mobile phones, and games consoles, are an important part of everyday life. We aim to empower students to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all our team including Directors, our team, tutors, support our team, external contractors, visitors, volunteers, and other individuals who work for, or provide services on behalf of Next Steps Education (collectively referred to as “our team” in this policy), as well as students, parents, and carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where students, our team or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

Links with other policies and practices

This policy links with several other policies, practices and action plans including Anti-bullying policy.

- Staff Code of Conduct
- Student Behaviour policy
- Safeguarding Policy
- GDPR Policy
- Any policies around curriculum, such as PSHE, RSE or Computing
- Mobile Phone Policy
- Cyber Security Policy

Technology in this area evolves and changes rapidly. This policy will be reviewed at least annually and following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure. Our Directors will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied, and to have oversight on any online safety concerns. Online safety, including incident reporting, filtering and monitoring, is a fixed item on weekly Director/ Team Meetings. Any issues identified via monitoring will be incorporated into our organisation action planning.

Roles and Responsibilities

The Designated Safeguarding Lead (DSL), Liz Fancourt (Director) and Sarah Logan (Director), has lead responsibility for online safety. Whilst activities of the DSL may be delegated to an appropriately trained deputy, overall, the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL.

Next Steps Education recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

All Directors will ensure online safety is a running and interrelated theme whilst devising and implementing our organisation's approach to safeguarding.

Our Directors will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety
- Ensure that suitable and appropriate filtering and monitoring systems are in place and monitor the safety and security of our systems and networks.
- Ensure that students are supported to develop an age-appropriate understanding of online safety.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local, and national support.
- Ensure that appropriate consideration and controls regarding the safe use of technology are included in student risk assessments.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Work with our team to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers, and the wider community, through a variety of channels and approaches.

The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of our team or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of our organisation's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of our team receive regular, up-to-date and appropriate online safety training.

- Access regular and appropriate training and support to ensure our team understand the unique risks associated with online safety and have the relevant up to date knowledge required to keep students safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that students with SEN and disabilities (SEND) face online.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Maintain records of online safety concerns, as well as actions taken, as part of our organisation's safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies, and procedures.

It is the responsibility of all members of our team to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in their teaching and mentoring sessions, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Know and contribute to Next Steps Education's filtering and monitoring process, where appropriate.

It is the responsibility of our Director managing the technical environment to:

- Provide technical support and perspective to the DSL, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures in partnerships with the DSL to ensure that our organisation's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.

- Ensure that our filtering and monitoring procedures are applied and updated on a regular basis
- Take appropriate safeguarding action if/when required.

It is the responsibility of students (at a level that is appropriate to their individual age and ability) to:

- Engage in age-appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Adhere to our policies, such as this policy and our mobile phone policy, as well as our Student Code of Conduct.
- Respect the feelings and rights of others, both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online.

It is the responsibility of parents and carers to:

- Encourage their children to adhere to safe use of the internet
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from Next Steps Education, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our available systems, such as learning platforms, and other network resources, safely and appropriately, as applicable.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Education and Engagement Approaches Education and engagement with students

Next Steps Education will raise awareness and promote safe and responsible internet use amongst students by:

- Ensuring education regarding safe and responsible use takes place alongside internet access.
- Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study (if applicable).
- Reinforcing online safety messages whenever technology or the internet is in use.

- Educating students in the effective use of the internet to research; including the skills of knowledge location, retrieval, and evaluation.
- Teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Next Steps Education will support students to understand our online safety policies in a way which suits their age and ability by:

- Displaying online safety posters in relevant areas in our Home Rooms.
- Informing students that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology.
- Implementing appropriate peer education approaches, where applicable.
- Providing online safety education as part of the transition programme into any online sessions or use of platforms provided by us.
- Seeking student voice when writing and developing online safety policies and practices, including curriculum development (where appropriate) and implementation.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

Vulnerable Students

Next Steps Education recognises that some students are more vulnerable online due to a range of factors. This may include, but is not limited to, children looked after (CLA) or children with a social worker (CIN), children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

Next Steps Education will differentiate online safety education, access and support as appropriate on an individual basis for vulnerable students.

Training and engagement with our team

Next Steps Education will:

- Provide and discuss the online safety policy and procedures with all members of our team as part of induction.
- Provide up-to-date and appropriate online safety training for all our team on a regular basis, with at least annual updates if applicable.
- This will cover the potential risks posed to students (Content, Contact, Conduct and Commerce), as well as our professional practice expectations.

- Recognise the expertise our team build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for our team to contribute to and shape online safety policies and procedures.
- Make our team aware that our IT systems are monitored, and that activity can be traced to individual users; our team will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make our team aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which our team should use, according to the age and ability of the students.
- Ensure all members of our team are aware of the procedures to follow regarding online safety concerns affecting students, colleagues, or other members of the community.

Awareness and engagement with parents and carers

Next Steps Education recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies. We will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats.
- Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
- Requesting that they read online safety information as part of joining our community, for example, within our Parent and Student Handbook.
- Requiring them to read our Online Safety Policy and discuss the implications with their children.

Reducing Online Risks

Next Steps Education recognises that the internet is a constantly changing environment with new apps, devices, websites, and material emerging at a rapid pace.

We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use within our organisation is encouraged.

- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material. (Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.)
- Make all members of our community aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of our community.

Safer Use of Technology within Sessions

Tutors and Mentors at Next Steps Education use a wide range of technology. This may include access to:

- Laptops
- Internet which may include search engines and educational websites
- Email
- Games consoles and other games-based technologies
- Digital cameras, web cams and video cameras.

- All setting owned devices will be used in accordance with our Cyber Security policies and with appropriate online safety and security measures in place.
- Members of our team will always evaluate websites, tools and apps fully before use in sessions or recommending for use at home.
- Members of our team will use age-appropriate search tools to identify which apps best suits the needs of each student.
- We will ensure that the use of internet-derived materials, by our team and students, complies with copyright law and acknowledge the source of information.
- Supervision of students will be appropriate to their age and ability.

Managing Internet Access

All our team members will read and sign this policy (or subsequent updates) as part of our onboarding process and annual training programme.

Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation. Full information can be found in our GDPR Policy.

Security and Management of Information Systems and Cyber Security

We take appropriate steps to ensure the security of our information systems, including:

- Protection against malware, viruses, phishing attacks, ransomware and other such security risks. See our Cyber Security Policy for full information.
- Not using portable media devices or hardware without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Blocking user-initiated downloads of unapproved software to work devices
- Advising against opening unfamiliar email attachments and quarantining suspicious emails for admin review.
- Regularly checking files held on our network
- Managing user logins and passwords accessing our network through organisation IT administration accounts.
- Asking all users to log off or lock their screens/devices if systems are unattended and having organisational IT global policies to enforce such behaviour.

Managing the Safety of our Website

We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.

- Students' personal information will not be published on our website.
- Our teams' personal contact information will not be published on our website.
- Contact details for Next Steps Education on the website will be our setting address, email and telephone number.
- Contact forms and data forms will use safe collection policies and block the ability to upload documents.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate and up-to-date information about safeguarding, including online safety, on our website for members of the community.
-

Publishing Images and Videos Online

We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

Managing Email

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, GDPR, (this) online safety and Staff/ Student Codes of Conduct.

- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- Next Steps Education email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of our community will immediately tell DSL if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use may be restricted.
- All members of our team are provided with Microsoft Teams accounts for official communication, and these are protected with MFA architecture.
- Members of our team are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between our team, students and parents.

Social Media and Our Team

The safe and responsible use of social networking, social media and personal publishing sites is evaluated and discussed when onboarding new team members.

- Safe use of social media is communicated via regular our team training opportunities.
- Safe and professional behaviour will be outlined for all members of our team (including volunteers) as part of our Code of Conduct.
- All members of our team are advised that their online conduct on social media can have an impact on their role and reputation as a tutor/ mentor.
- Civil, legal or disciplinary action may be taken if our team are found to bring the profession or Next Steps Education into disrepute, or if something is felt to have undermined confidence in their professional abilities.

- All members of our team are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to our team via our team training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Setting the privacy levels of their personal sites.
- Being aware of location sharing services.
- Opting out of public listings on social networking sites.
- Logging out of accounts after use.
- Keeping passwords safe and confidential.
- Ensuring our team do not represent their personal views as those of Next Steps Education.

- All members of our team are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that our team members have access to as part of their employment, including photos and personal information about students and their family members or colleagues will not be shared or discussed on social media sites.
- Members of our team will notify the Directors immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with students and parents and carers

All members of our team are advised not to communicate with or add as 'friends' any current or past students or their family members via any personal social media sites, applications or profiles.

- If ongoing contact with students is required once they have left the setting, members of our team will be expected to use official setting provided communication tools.
- Our team will not use personal social media accounts to contact students or parents, nor should any contact be accepted.
- Any communication from students and parents received on personal social media accounts will be reported to the DSL (or deputy).

Students' Personal Use of Social Media

Safe and appropriate use of social media will be taught to students where opportunities arise as part of an embedded and progressive education approach, via age-appropriate sites and resources. Any concerns regarding students' use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour. Students do not currently have access to smart phones or other technology whilst in our Home Rooms and are encouraged to not have visible phones during any tuition or mentoring sessions. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

Students will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns (to our team members, on our website and externally).

Our team expectations

Members of our team who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries. If members of our team are participating in online social media activity as part of their capacity as a team member of Next Steps Education, they will:

- Agree to our online safety policy.
- Always be professional and aware they are an ambassador for Next Steps Education.
- Disclose their official role and/or position but make it clear that they do not necessarily speak on behalf of Next Steps Education.
- Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.

- Ensure that they have appropriate consent (from parents and from Directors) before sharing images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of Next Steps Education, unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, students, parents and carers.
- Inform the Directors of any concerns, such as criticism, inappropriate content or contact from students.

Use of Mobile and Smart Technology

Next Steps Education recognises that personal communication through mobile technologies is an accepted part of everyday life for students, our team and parents/carers, but technologies need to be used safely and appropriately within the setting.

Expectations

All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.

Electronic devices of any kind that are brought onto site are the responsibility of the user.

All members of Next Steps Education community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.

All members of the Next Steps Education community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

Mobile phones and personal devices are not permitted to be visible in our tuition sites, such as The Home Rooms (Bideford).

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Code of Conduct.

All members of Next Steps Education are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our Code of Conduct or Safeguarding policies.

All members of Next Steps Education are reminded that taking covert images typically under clothing (upskirting) is illegal and will be dealt with as part of the Staff Code of Conduct.

Our team Use of Mobile and Smart Technology

Members of our team will ensure that use of personal phones and devices takes place in accordance with the law, as well as relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.

Our team will be advised to:

- Keep mobile phones and personal devices in a safe and secure place during session times.
- Keep mobile phones and personal devices switched off or switched to 'silent' mode during session times.
- Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during session times.
- Not use personal devices during tuition/ mentoring sessions, unless permission has been given by the Directors, such as in emergency circumstances.
- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

Members of our team are NOT permitted to use their own personal phones or devices for contacting students.

Our team will not use personal devices:

- To take photos or videos of students and will only use work-provided equipment for this purpose.
- Directly with students and will only use work-provided equipment during lessons/educational activities.

If a member of our team breaches our policy, action will be taken in line with our Code of Conduct.

If a member of our team is thought to have illegal content saved or stored on a mobile phone or personal device, or have committed a criminal offence, the police will be contacted.

Students' Use of Mobile and Smart Technology

Students will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

Visitors' Use of Mobile and Smart Technology

Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our Mobile Phone Policy. We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use. Members of our team are expected to challenge visitors if they have concerns and will always inform the Directors of any breaches our policy.

Responding to Online Safety Incidents and Concerns

All members of our community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

All members of our community must respect confidentiality and the need to follow the official procedures for reporting concerns. Students, parents and our team will be informed of our Complaints Policy and our team will be made aware of the Whistleblowing Policy.

We require our team, parents, carers and students to work in partnership to resolve online safety issues. After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

If an incident or concern needs to be passed beyond our community (for example, if other local settings are involved or the public may be at risk), the DSL will speak with Devon & Cornwall Police first to ensure that potential investigations are not compromised.

Concerns about Students' Welfare

The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns and will record these issues in line with our Safeguarding Policy. The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies. We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

Our Team Misuse

Any complaint about our team misuse will be referred to the Directors in accordance with the safeguarding policy. Issues which do not meet the threshold requiring reporting to the LADO will be recorded in our record of low-level concerns. Any allegations regarding a member of our team's online conduct reaching the threshold will be discussed with the LADO (Local Authority Designated Officer). Appropriate action will be taken in accordance with our Code of Conduct.

Procedures for Responding to Specific Online Incidents or Concerns

Online Sexual Violence and Sexual Harassment between Children

All team members at Next Steps Education have read and understood the guidance and part 5 of 'Keeping Children Safe in Education' 2025.

We recognise that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation. Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our Safeguarding Policy.

We recognise that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities. We also recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

We will ensure that all members of our community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by making available a range of age and ability appropriate educational methods.

We will ensure that all members of our community are aware of sources of support regarding online sexual violence and sexual harassment between children.

We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment. If made aware of online sexual violence and sexual harassment, we will:

- Immediately notify the DSL (or deputy) and act in accordance with our
- Safeguarding Policy.
- If content is contained on students' electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- Provide the necessary safeguards and support for all students involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate pastoral support.
- Implement appropriate sanctions in accordance with our Student Code of Conduct.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make a referral to partner agencies, such as MASH and/or the Police.

- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
- If a criminal offence has been committed, the DSL (or deputy) will discuss this with Devon & Cornwall Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Youth Produced Sexual Imagery ("Nudes")

We recognise youth produced sexual imagery (known as "nudes") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

This section only applies to YP under the age of 18 creating/sharing/receiving nudes of a YP. It does not apply to children sharing adult pornography.

On any occasion when an adult is in possession of or is sharing an illegal image of a YP – this will always be an urgent police matter. We will follow the advice set out by the DfE.

- We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

Online Child Sexual Abuse and Exploitation

We will ensure that all members of our community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

We recognise online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).

Schools are reminded that a criminal offence has been committed if a person aged 18 or over intentionally communicates with a child under 16, who the adult does not reasonably believe to be 16 or over, if the communication is sexual or if it is intended to encourage the child to make a communication which is sexual. The offence will be committed whether or not the child communicates with the adult. This is the offence of sexual communication with a child under section 67 of the Serious Crime Act 2015.

We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for students, our team and parents/carers.

We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.

We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using our provided or personal equipment.

If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the MASH or Devon & Cornwall Police.

If students at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Devon & Cornwall Police and/or MASH first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

We will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.

We will seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Devon & Cornwall Police and/or the MASH.

If made aware of IIOC, we will:

- Act in accordance with our child protection policy and the relevant procedures.
- Store any devices involved securely.
- Immediately inform appropriate organisations, such as CEOP, Devon & Cornwall Police or the LADO.

If made aware that a member of our team or a student has been inadvertently exposed to indecent images of children, we will:

- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation.
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on our provided devices, we will:

- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation.
- Ensure that any copies that exist of the image, for example, in emails, are deleted.
- Inform the Police via 101 (999 if there is an immediate risk of harm) and First Contact
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

If made aware that a member of our team is in possession of indecent images of children on setting provided devices, we will:

- Ensure that the Directors are informed in line with our managing allegations against our team policy.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against our team policy.
- Quarantine any devices until police advice has been sought.

Child Criminal Exploitation – Including County Lines

All our team need to be aware of the indicators that a child may be at risk from, or involved with Child Criminal Exploitation (CCE) and note that this can be facilitated through the use of technology. Further details are in our Safeguarding Policy.

Cyberbullying and Online Hate

Cyberbullying, along with all other forms of bullying, will not be tolerated at Next Steps Education. Online hate content, directed towards or posted by, specific members of our community will not be tolerated at Next Steps Education and will be responded to in line with existing policies, including our Student Code of Conduct.

All members of our community will be advised to report online hate in accordance with relevant policies and procedures. The Police will be contacted if a criminal offence is suspected. If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through MASH or Devon & Cornwall Police Online

Radicalisation and Extremism

We will take all reasonable precautions to ensure that students and our team are safe from terrorist and extremist material when accessing the internet on site. If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our Safeguarding Policy.

If we are concerned that a member of our team may be at risk of radicalisation online, the Directors will be informed immediately, and action will be taken in line with our Safeguarding and Staff Code of Conduct policies.

Artificial Intelligence (AI)

Next Steps Education understand the valuable potential that artificial intelligence (AI), including generative AI, holds for education. For example, it can be used to enhance pedagogical methods, customise learning experiences and progress educational innovation. We are also aware of the risks posed by AI, including data protection breaches, copyright issues, ethical complications, safeguarding and compliance with wider legal obligations. We aim to establish guidelines for the ethical, secure and responsible use of AI technologies by our team and students. This includes generative chatbots such as ChatGPT and Google Gemini (please note, this list is not exhaustive) and both open and closed AI generative tools.

- Open generative AI tools are accessible and modifiable by anyone. They may store, share or learn from the information entered into them, including personal or sensitive information
- Closed generative AI tools are generally more secure, as external parties cannot access the data you input

This policy reflects good practice guidelines/recommendations in the following publications:

- AI regulation white paper, published by the Department for Science, Innovation and Technology, and the Office for Artificial Intelligence
- Generative artificial intelligence (AI) and data protection in schools, published by the Department for Education (DfE) This policy also meets the requirements of the:
- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018) 3.

Next Steps Education will:

- Support the use of AI to enhance teaching and learning
- Support our team to explore AI solutions to improve efficiency and reduce workload
- Prepare our team, governors and students for a future in which AI technology will be an integral part
- Promote equity in education by using AI to address learning gaps and provide personalised support
- Ensure that AI technologies are used ethically and responsibly by our team and students
- Protect the privacy and personal data of our team and students in compliance with the UK GDPR

We follow the 5 principles set out in the AI regulation white paper:

Safety, security and robustness

- Ensure that AI solutions are secure and safe for users and protect users' data
- Ensure we can identify and rectify bias or error
- Anticipate threats such as hacking

Appropriate transparency and explainability

- Be transparent about our use of AI, and make sure we understand the suggestions it makes

Fairness

- Only use AI solutions that are ethically appropriate, equitable and free from prejudice – in particular, we will fully consider any bias relating to small groups and protected characteristics before using AI, monitor bias closely and correct problems where appropriate

Accountability and governance

- Ensure that the Directors and our team have clear roles and responsibilities in relation to the monitoring, evaluation, maintenance and use of AI

Contestability and redress

- Make sure that our team are empowered to correct and overrule AI suggestions – decisions should be made by the user of AI, not the technology
- Allow and respond appropriately to concerns and complaints where AI may have caused error resulting in adverse consequences or unfair treatment

The Directors are responsible for the day-to-day leadership, ownership and management of generative AI used for education and productivity within the scope of Next Steps Education work. Directors will:

- Hold themselves to account for the implementation of AI, in line with this AI policy.
- Ensure appropriate support to make informed decisions regarding the effective and ethical use of AI in Next Steps Education.
- Adhere to the guidelines below to protect data when using generative AI tools:
- Use only approved AI tools (see section 5)
- Seek advice from external consultants, as appropriate
- Check whether they are using an open or closed generative AI tool
- Ensure there is no identifiable information included in what they put into open generative AI tools
- Acknowledge or reference the use of generative AI in their work
- Fact-check results to make sure the information is accurate
- Ensure that the use of AI is in accordance with data protection legislation
- Ensure that the guidance set out in this policy is followed by all our team
- Review and update this AI policy as appropriate, and at least annually
- Ensure our team are appropriately trained in the effective use and potential risks of AI
- Give students opportunities to learn about the effective use and potential risks of AI

- Evaluate and approve uses of AI, or new AI tools, taking into account data protection impact assessments and referring to our GDPR Policy
- Monitor our compliance with safeguarding requirements, including in relation to the use of AI, such as:
- Being aware of new and emerging safeguarding threats posed by AI
- Updating and delivering our team training on AI safeguarding threats
- Responding to safeguarding incidents in line with Keeping Children Safe in Education (KCSIE)

As part of our aim to reduce our team workload while improving outcomes for our students, we encourage our team to explore opportunities to meet these objectives through the use of approved AI tools. Any use of AI must follow the guidelines set out in this policy. To protect data when using generative AI tools, our team must:

- Use only approved AI tools (see section 5)
- Seek advice from the Director responsible for Online & Tech Safety
- Check whether they are using an open or closed generative AI tool
- Ensure there is no identifiable information included in what they put into open generative AI tools
- Acknowledge or reference the use of generative AI in their work
- Fact-check results to make sure the information is accurate

All our team play a role in ensuring that students understand the potential benefits and risks of using AI in their learning. All our team have a responsibility to guide students in critically evaluating AI-generated information and understanding its limitations.

Students must:

- Follow the guidelines set out in section 7 of this policy (‘Use of AI by students’)

Always consider whether AI is the right tool to use. Just because the Directors of Next Steps Education have approved its use doesn’t mean it will always be appropriate. Given how rapidly AI is evolving, please note Next Steps Education will keep an updated list of approved new AI tools

Approved AI tools

Gamma

Arbor AI

Gemini

Chat GPT

Claude 3

Copilot

Notebook LM

TeacherGENie

Approved uses

- Letter to parents/carers
- Job descriptions and adverts
- Interview questions
- Creating slides for teaching/mentoring sessions
- Emails, SMS, Letters
- Support with research, lesson plans, writing emails and letters
- Newsletters
- Analysing anonymous data
- Creating images to aid with learning
- Supporting learning through extending questions based on existing nuggets.

Our Directors welcome suggestions for new ways to use AI to improve student outcomes and reduce workload. Our team should contact the Directors to discuss any ideas they may have with regards to using AI for evaluation.

Intellectual property

Most generative AI tools use inputs submitted by users to train and refine their models. Students own the intellectual property (IP) rights to the original content they create. This is likely to include anything that shows working out or is beyond multiple choice questions. Students' work must not be used by our team to train generative AI models without appropriate consent or exemption to copyright. Exemptions to copyright are limited – we will seek legal advice if we are unsure as to whether we are acting within the law.

Bias

We are aware that AI tools can perpetuate existing biases, particularly towards special characteristics including sex, race and disability. This means that critical thought must be applied to all outputs of authorised AI applications. This means fact and sense-checking the output before relying on it. We will ensure we can identify and rectify bias or error by training our team in this area. We also regularly review our use of AI to identify and correct any biases that may arise. If parents/carers or students have any concerns or complaints

about potential unfair treatment or other negative outcomes as a consequence of AI use, these will be dealt with through our usual complaints policy & procedure.

Raising concerns

We encourage our team to speak to the Directors in the first instance if they have any concerns about a proposed use of AI, or the use of AI that may have resulted in errors that lead to adverse consequences or unfair treatment.

Ethical and responsible use

We will always:

- Use generative AI tools ethically and responsibly
- Remember the principles set out in our school's equality policy when using generative AI tools
- Consider whether the tool has real-time internet access, or access to information up to a certain point in time, as this may impact the accuracy of the output
- Fact and sense-check the output before relying on it

Our team must not:

- Generate content to impersonate, bully or harass another person
- Generate explicit or offensive content
- Input offensive, discriminatory or inappropriate content as a prompt

Educating students about AI

Next Steps Education acknowledges that students benefit from a knowledge-rich curriculum that allows them to become well-informed users of technology and understand its impact on society. Strong foundational knowledge will ensure that students develop the right skills to make the best use of generative AI. Students are taught in the curriculum about the potential benefits of using AI tools to aid their learning, while also covering subjects such as:

- Creating and using digital content safely and responsibly
- The limitations, reliability and potential bias of generative AI
- How information on the internet is organised and ranked
- Online safety to protect against harmful or misleading content

Use of AI by students

We recognise that AI has many uses to help students learn. Students may use AI tools:

- As a research tool to help them find out about new topics and ideas

- When specifically studying and discussing AI in sessions, for example in IT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed and appropriate for the students' age and educational needs.

AI may also lend itself to cheating and plagiarism. To mitigate this, students may not use AI tools:

- During assessments, including internal and external assessments, and coursework
- To write their homework or assignments, where AI-generated text is presented as their own work
- To complete their homework, where AI is used to answer questions set and is presented as their own work (for example, maths calculations). This list of AI misuse is not exhaustive. Where AI tools have been used as a source of information, students should reference their use of AI. The reference must show the name of the AI source and the date the content was generated.

- Students must consider what is ethical and appropriate in their use of AI and must not:
  - Generate content to impersonate, bully or harass another person
  - Generate explicit or offensive content
  - Input offensive, discriminatory or inappropriate content as a prompt

Formal assessments

We will continue to take reasonable steps where applicable to prevent malpractice involving the use of generative AI in assessments. We will follow the latest guidance published by the Joint Council for Qualifications (JCQ) on AI use in assessments.

Our team training

Our team will be kept up to date with developments in AI, and how they will be able to develop and improve their practice on a regular basis:

- How you ensure good understanding of AI
- Who will be responsible for ensuring our team have access to continuing professional development (CPD) opportunities on AI
- How Next Steps Education will stay abreast of good practice and what mechanisms you have in place for sharing it

Breach of this policy by our team

Breach of this policy by our team will be dealt with in line with our Staff Code of Conduct. Where disciplinary action is appropriate, it may be taken whether the breach occurs:

- During or outside of working hours
- On an individual's own device or a Next Steps Education owned device
- At home, at our Home Rooms or from a remote working location

Our team members will be required to co-operate with any investigation into a suspected breach of this policy. This may involve providing us with access to:

- The generative AI application in question (whether or not it is one authorised by Next Steps Education)
- Any relevant passwords or login details
- Team members must report any breach of this policy, either by themselves or by another member of our team, to the Directors as soon as possible.

Breach of this Policy by students

Any breach of this policy by a student will be dealt with in line with our Student Code of Conduct

Monitoring and transparency

AI technology, and the benefits, risks and harms related to it, evolves and changes rapidly. Consequently, this policy is a live document that must be kept updated by the Directors.

This policy will also be regularly reviewed and updated to align with emerging best practices, technological advancements and changes in regulations. All our team are expected to read and follow this policy. Our Directors will monitor the effectiveness of AI usage across the school. We will ensure we keep members of our community up to date on the use of AI technologies for educational purposes. As part of our regular surveys, feedback from students, parents/carers and our team will be considered in the ongoing evaluation and development of AI use in school.

Useful Links for Online Safety and AI Use in Educational Settings

- https://www.ceop.police.uk/Safety-Centre/
- https://saferinternet.org.uk/resource/thinkuknow-advice-from-ceop
- https://www.childnet.com
- www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- Parent Protect https://www.parentsprotect.co.uk (advice for parents on peer-on-peer abuse and how to cope if your child has got into significant trouble online)
- NSPCC: www.nspcc.org.uk/onlinesafety
- ChildLine: www.childline.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

- 360 Safe Self-Review tool: https://swgfl.org.uk/services/360-degree-safe/
- Parentzone https://parentzone.org.uk/
- Internet Matters: https://www.internetmatters.org (particularly useful for providing clear information and up-to-date advice on setting parental controls).
- Action Fraud: https://www.actionfraud.police.uk (This is the place to report ransomware, scams etc.)
- Get Safe Online: https://www.getsafeonline.org
- Net Aware: https://www.net-aware.org.uk