NEWTON INTERNATIONAL ACADEMY

SMASH

ONLINE SAFETY AND DIGITAL CITIZENSHIP POLICY

POLICY REVIEWED

July 2026

POLICY TO BE REVIEWED

July 2027

ONLINE SAFETY and DIGITAL CITIZENSHIP POLICY

Updated July 2026

Updated by S Hardy

Review July 2027

For Staff and Parent issue

This policy applies to the whole school, including the Early Years Foundation Stage and takes in to account safe practice as set out by the following;

DfE *Keeping Children Safe in Education (KCSIE 2025)*
UKCIS *Education for a Connected World*
BSO inspection expectations
CIS Accreditation Standards (Safeguarding, Wellbeing and Digital Citizenship)

Policy Introduction and Aims

The internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. However, these modern technologies have created a landscape of challenges and dangers that is still constantly changing. Online safety is recognised as a safeguarding issue and is approached in line with Keeping Children Safe in Education (KCSIE). The school acknowledges that technology is a significant component in many safeguarding and wellbeing concerns and therefore adopts a whole-school approach to online safety.

Newton International Academy Smash recognises that children may experience risks online through content, contact, conduct and commerce, and that these risks may occur through social media, gaming platforms, messaging applications, artificial intelligence tools, wearable technologies, smart devices and emerging technologies. Online safety education aims not only to protect pupils but also to empower them to become responsible, ethical and resilient digital citizens.

In order to ensure that the school provides a safeenvironment for learning, we adhere to the following principles:

- Online safety is an essential part of safeguarding, and the school has a duty to ensure that all pupils and staff are protected from potential harm online

- Online safety education is an important preparation for life. Pupils should be empowered to build resilience and to develop strategies to prevent, manage and respond to risk online

This policy applies to all staff including teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers. It applies to the whole school, including the Early Years Foundation Stage. It applies to access to school systems, the internet and the use of technology, using devices provided by the school or personal devices.

The policy also applies to online safety behaviour such as cyber-bullying, which may take place outside the school, but is linked to membership of the school. The school will deal with such behaviour within this policy and associated behaviour and discipline policies, and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school.

The purpose of the online safety policy is to:

- Safeguard and protect all members of the school's community online
- Identify approaches to educate and raise awareness of online safety throughout the community
- Enable all staff to work safely and responsibly, to 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.

The issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

Content: being exposed to illegal, inappropriate or harmful material; for example, racist or radical andextremist views, and in some respects fake news.
Contact: being subjected to harmful online interaction with other users; for example, children canbe contacted by bullies or people who groom or seek to hurt them.
Commercial exploitation: for example, young people can be unaware of hidden costs and advertising in apps, games, and websites.
Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving images, or online bullying.

Responsibility

The Principal is responsible for ensuring online safety is a key priority within the school. The Principal, along with the Senior Management and Staff members;

- Ensures that online safety is viewed as a safeguarding issue and that practice is in line with school and national recommendations and requirements
- Ensures the school follows policies and practices regarding online safety (including the Acceptable Use Agreements), information security and data protection
- Ensures that online safety is embedded within the whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety
- Ensures that all staff receive regular, up to date and appropriate online safety training
- Is aware of what to do in the event of a serious online safety incident, and will ensure that there are robust reporting channels for online safety concerns, including internal, school and national support

- Ensures that all staff receive regular, up to date and appropriate online safety training
- Is aware of what to do in the event of a serious online safety incident, and will ensure that there are robust reporting channels for online safety concerns, including internal, school and national support

- Receives reports from the Designated Safeguarding team on online safety

- Ensures that online safety practice is audited and evaluated regularly in order to identify strengths and areas for improvement.

The Designated Safeguarding Leads (DSL and DDSLs):

- Take day to day responsibility for online safety
- Promote an awareness of and commitment to online safety throughout the school community
- Act as the named point of contact on all online safety issues
- Facilitates training and advice for all staff, keeping colleagues informed of current research, legislation and trends regarding online safety and communicating this to the school community, as appropriate
- Maintains the online safety incident log and record of actions taken, and reviews the log periodically to identify gaps and trends
- Reports regularly to Principal and SLT on the incident log, internet monitoring, current issues, developments in legislation.
- The DSL team will ensure that online safety is fully integrated into safeguarding procedures and that online safety concerns are recorded, monitored and responded to in line with child protection procedures.
- The DSL team will maintain awareness of emerging technologies including Artificial Intelligence (AI), wearable technology, smart devices and online platforms that may pose safeguarding risks.
- The DSL team will work with IT staff to regularly review filtering and monitoring systems in accordance with DfE Filtering and Monitoring Standards.

Staff responsible for the Technical Environment:

- Apply appropriate technical and procedural controls to ensure that the school's IT infrastructure system is secure.

- Keep up to date with the school's online safety policy and technical information in order to carry out their online safety role effectively and to inform and update others as relevant.

- Are aware of what to do in the event of a serious online safety incident, and will ensure that there are robust reporting channels for online safety concerns, including internal, school and national support.

- Provide technical support to the DSL and leadership team in the implementation of online safety Procedures.

- Ensure that the school's filtering policy is applied and updated on a regular basis, and oversees the school's monitoring system.

- Report any filtering breaches or other online safety issues to the DSL, Head and Principal as appropriate.

- Ensure that any safeguarding concerns are reported to the DSL, in accordance with the school's safeguarding procedures.

All school staff:

- Read, adhere to, and help promote the online safety policy, *Acceptable Use Agreements* and other relevant school policies and guidance
- Take responsibility for the security of school systems and the data they use, or have access to
- Model safe, responsible, and professional behaviours in their own use of technology
- Embed online safety in their teaching and other school activities
- Supervise, guide and monitor pupils carefully when engaged in activities involving online technology (including extra-curricular and extended school activities if relevant)
- Have an up-to-date 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 reporting to the DSL
- Know when and how to escalate online safety issues
- Take personal responsibility for professional development in this area.

Pupils (at a level that is appropriate to their individual age, ability and vulnerabilities):

- Engage in age-appropriate online safety education opportunities.
- Read and adhere to the school *Acceptable Use Agreement.*
- Respect the feelings and rights of others both on and offline, in and out of school.
- Take responsibility for keeping themselves and others safe online.
- Report to a trusted adult if there is a concern online.

Parents and Carers:

- Read the school *Acceptable Use Agreements* and encourage their children to adhere to them
- Support the school in online safety approaches by discussing online safety issues with their children and reinforcing appropriate, safe online behaviours at home
- Model safe and appropriate use of technology and social media, including seeking permission before taking and sharing digital images of pupils other than their own children
- Identify changes in behaviour that could indicate that their child is at risk of harm online

- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online
- Use school systems, such as learning platforms, and other network resources, safely and appropriately
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Education and Engagement

Education and engagement with pupils

The school curriculum includes age-appropriate lessons and activities on online safety for all pupils, intended to raise awareness, build resilience and promote safe and responsible internet use by:

- Ensuring pupil education adheres to safe and responsible use of the internet.
- Including online safety across the curriculum, including the PSHE, and Computing programmes of study, covering use both at school.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Ensuring that the needs of pupils considered to be more vulnerable online, (SEND or mental health needs) are met appropriately.
- Using support, such as peer education approaches and external visitors, to complement online safety education in the curriculum.
- Educating pupils in the effective use of the internet to research; including the skills of knowledge,location, retrieval, and evaluation.
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Teaching pupils to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Supporting students in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision- making.

The school will support pupils to read and understand the *Acceptable Use Agreement (AUA)* in a way which suits their age and ability by:

- Discussing the AUA and its implications, and reinforcing the principles via display, classroom discussion etc.
- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation
- Recognising positive use of technology by pupils.

Training and Engagement with Staff

Newton International Academy Smash will:

• Provide and discuss the *Online Safety Policy* and staff *Acceptable Use Agreement* with all members of staffas part of induction.

• Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annualupdates.

• Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.

• Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school

• Highlight useful educational resources and tools which staff should use, according to the age and ability ofthe pupils.

• Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

Awareness and engagement with Parents and Carers

Parents and carers have an essential role to play in enabling children to become safe and responsible usersof the internet and associated technologies. The school 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. This will include offeringspecific online safety awareness training and highlighting online safety at other events such as parent evenings
- Drawing parents' attention to the school online safety policy and expectations in newsletters andon the website
- Requiring parents to read the pupil *Acceptable Use Agreement* and discuss its implications with theirchildren.

Reducing Online Risks

The internet is a constantly changing environment with new apps, devices, websites and material emergingat a rapid pace. The school 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 in school is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Ensure, through online safety education and the school acceptable usage agreement, that pupils know that the school's expectations regarding safe and appropriate behaviour online apply whether the school's networksare used or not.

Emerging Technologies

NIA Smash recognises that new technologies can create additional safeguarding risks. These include but are not limited to:

- Artificial Intelligence (AI) platforms
- Smart watches
- Fitness trackers
- Wearable cameras
- Smart glasses
- Voice activated devices
- Location-sharing applications
- Virtual reality and augmented reality platforms
- Live-streaming applications

Risk assessments will be undertaken before new technologies are introduced into the curriculum or wider school environment. The school will regularly review technological developments to ensure that safeguarding arrangements remain effective.

Safer Use of Technology

Classroom Use

The school uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Internet which may include search engines and educational websites
- Learning platforms
- Cloud services and storage
- Email and messaging
- Games consoles and other games-based technologies
- Digital cameras, web cams and video cameras
- Virtual reality headsets

Supervision of pupils will be appropriate to their age and ability. All school-owned devices should be used in accordance with the school's AUAs and with appropriate safety and security measures in place. Members of staff should always check websites, tools and apps for suitability before use in the classroom or recommending for use at home.

Filtering and Monitoring

• All incoming data is screened by an application that provides real-time filtering and protects both networksand users from internet threats.

It prevents a wide range of unwelcome material and malware from being available in schools while at the same time allowing access to material of educational value. The policy determining filtering is managed centrally, with different levels being applied depending on age group

• The system logs all internet access on school devices, and these logs can be accessed by the DSL for monitoring purposes. Flagged terms will also trigger alerts which the DSL may investigate. Concernsidentified will be managed according to the nature of the issue

• All members of staff are however aware that they cannot rely on filtering and monitoring alone to safeguard pupils: effective classroom management and regular education about safe and responsible use isessential

- All users are informed that use of school systems is monitored and that all monitoring is in line with data protection, human rights and privacy legislation.
- Filtering and monitoring systems will be reviewed regularly by senior leaders, safeguarding leaders and technical staff to ensure that they remain effective and proportionate.
- Staff understand that filtering and monitoring are important safeguarding tools but do not replace active supervision, professional curiosity and effective safeguarding practice.

Dealing with Filtering breaches

The school has a clear procedure for reporting filtering breaches:

- If pupils discover unsuitable sites, they will be required to alert a member of staff immediately.
- The member of staff will report the concern (including the URL of the site if possible) to the DSL.
- The breach will be recorded and escalated as appropriate.

Social Media

Expectations

- The term social media includes (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chat rooms and instant messenger.
- All members of the school community are expected to engage in social media in a positive, safe, and responsible manner, at all times.

Staff Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites are discussedwith all members of staff as part of staff induction and is revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour is outlined for all members of staff as part of the staff *Code of Conduct*, staff *Acceptable Use Agreement* and *Social Media Policy.*

Pupils' Personal Use of Social Media

Safe and appropriate use of social media will be taught to pupils as part of online safety education,via age-appropriate sites and resources. The school is aware that many popular social media sites state that they are not for children under the age of 13. The school will not create accounts specifically for children under this age. The school will control pupil access to social media whilst using school-provided devices and systems on site.

The use of social media during school hours for personal use is not permitted.

Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary action and/or removal of internet facilities.
Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with

existing school policies. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

Mobile Phones, Wearable Technology and Recording Devices

The school recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriatelywithin school.

Wearable Technology and Recording Devices

Wearable technology includes, but is not limited to, smart watches, smart glasses, fitness trackers, wearable cameras and any device capable of recording audio, images, video or transmitting data.Wearable devices capable of recording images, audio or video must not be used by pupils during the school day without explicit permission from a member of staff. Any unauthorised recording of pupils, staff or visitors may result in disciplinary action and may be treated as a safeguarding concern. The use of wearable devices is prohibited in toilets, changing areas, medical rooms and any location where privacy is expected. The school reserves the right to request the removal or secure storage of wearable devices where safeguarding concerns arise. Staff must not use personal devices, wearable technology or recording equipment to capture images, audio or video of pupils unless authorised and in accordance with safeguarding and data protection procedures. This addition is particularly important because UK safeguarding guidance increasingly references covert recording, smart watches and wearable technology risks.

Expectations

All use of personal devices and mobile phones will take place in accordance with appropriate school policies, including, but not limited to: *Anti-Bullying*, *Behaviour and Discipline*, and *Safeguarding and Child Protection*. Electronic devices of any kind that are brought onto site are the responsibility of the user at alltimes. The school accepts no responsibilities for the loss, theft, damage, or breach of security ofsuch items on school premises. Mobile phones and personal devices are not permitted to be used in specific areas within the school sitesuch as changing rooms, toilets and swimming pools. Mobile phones should be put away in lockers / not used in school or on the school site. The sending of abusive or inappropriate messages/content via mobile phones or personal devices isforbidden by any member of the community; any breaches will be dealt according to the school behaviour policy.

- All members of the community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school behaviour or *Safeguarding and Child Protection* policies.

Staff Use of Personal Devices and Mobile Phones

Members of staff will ensure that the use of personal phones and devices takes place in accordance with the law, as well as relevant school policy and procedures, such as: *Safeguarding and Child Protection*, and *Acceptable Use Agreements*. Images of pupils (other than a member of staff's own children) must not be stored on personal devices. Any image taken on personal devices must be transferred to school systems as soon as reasonably possible and the personal copy permanently removed.

Pupil's use of personal devices and Mobile phones

Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones andwill be made aware of boundaries and consequences. Pupil's personal devices and mobile phones are expected to be kept in a secure place, switched off, or kept out of sight during lessons and while moving between lessons.

If a pupil needs to contact his/her parents or carers they will be allowed to use their mobile phone or a school phone, as long as they have permission from a member of school staff.

The default will be however to go to the school office and for the call to be made by a member of the officeteam. Parents are advised to contact their child via the school office during school hours rather than via students' personal phones.

Mobile phones or personal devices will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff. Mobile phones and personal devices must not be taken into examinations. Pupils found in possession of amobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the pupil's grade in that examination being nullified.

If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place and only released to a Parent / Carer.

Schools are not required to inform parents before a search takes place or to seek consent for a search fora prohibited item, or item which a member of staff reasonably suspects has been or is likely to be used to commit an offence or to cause personal injury or damage to the property of any person.

Where the person conducting the search finds an electronic device that is prohibited by the school rules or that they reasonably suspect has been, or is likely to be, used to commit an offence or cause personal injury or damage to property, they may examine any data or files on the device where there is a good reasonto do so. They may also delete data or files if they think there is a good reason to do so, unless they are going to give the device to the police.

If there is a suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation. The confiscation and searching of a phone or other digital device will normally be carried out inconsultation with a senior member of staff.

Visitor's Use of Personal Devices and Mobile Phones

Parents, carers, and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's *Acceptable Use Agreement* and other associated policies, such as *Anti-Bullying* and *Safeguarding and Child Protection policies.*

The school will ensure appropriate signage and information is provided to inform parents, carersand visitors of expectations of use.

Concerns about Pupils' Welfare

The DSL will be informed immediately of any online safety incident that could be considered a safeguardingor child protection concern.

The school will inform parents and carers of any incidents or concerns involving their child, as andwhen required.

Misuse

- Complaints about IT misuse by pupils will be dealt with by a senior member of staff under the relevant policies and procedures and according to the nature of the complaint

- Any complaint about staff misuse will be referred to the Principal

- Pupils and parents are informed of the school's complaints procedure.

Use of Artificial Intelligence (AI)

The school recognizes the increasing role of Artificial Intelligence (AI) in education, including tools that support learning, assessment, communication, and administrative functions. While AI can offer valuable educational benefits, it also presents risks that must be carefully managed to ensure the safety, privacy, and well-being of students and staff.

Responsible Use of AI Tools

- AI tools may be used to support teaching and learning, such as chatbots, tutoring systems, and content generation tools.
- Staff and students must use AI tools responsibly and in accordance with the school's acceptable use policy.
- AI-generated content should be clearly identified, and students should not present AI-generated work as entirely their own without attribution.

Data Privacy and Protection

- AI systems that collect or process student or staff data must comply with data protection regulations (e.g. GDPR).
- Personal information should not be entered into AI tools unless those tools have been approved by the school and are compliant with privacy policies.

Digital Literacy and Critical Thinking

- The school will educate students on how to use AI tools safely, ethically, and effectively.
- Students will be taught to evaluate the accuracy, reliability, and potential bias of AI-generated content.

Safeguarding Risks associated with AI

- AI tools used within the school environment may be monitored to ensure they are being used appropriately.
- AI systems will not replace human judgment in matters of safeguarding or discipline. Final decisions will always involve appropriate school staff.
- The school recognises that AI tools may expose users to inaccurate, misleading, biased or inappropriate content.
- AI platforms may be used to generate realistic images, audio and video (deepfakes). Pupils will be educated about the risks associated with manipulated digital content and how to report concerns.
- The creation, sharing or possession of AI-generated harmful content involving members of the school community will be treated as a safeguarding concern and managed in accordance with the Safeguarding and Child Protection Policy.
- Staff must not upload confidential, sensitive or personal information relating to pupils, parents or staff into public AI systems unless specifically authorised and compliant with school data protection requirements.

AI and Online Risks

- Students will be made aware that some AI tools available online may produce harmful, inappropriate, or misleading content.
- The school will provide guidance on identifying and avoiding unsafe or untrustworthy AI platforms.

Child-on-Child Online Abuse

At NIA Smash we recognise that online abuse can occur between children and may include:

- Cyberbullying
- Sexual harassment
- Sexualised comments
- Sharing of nude or semi-nude images
- Coercion
- Online exploitation
- Use of AI-generated sexual imagery
- Threatening or abusive online behaviour

Incidents will be managed in line with the Safeguarding and Child Protection Policy and Child-on-Child Abuse procedures.

Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, youth produced sexual imagery (sexting), cyber bullying and illegalcontent.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
- Incidents will be managed depending on their nature and severity, according to the relevant school policies.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes in policy or practice as required.

Monitoring and Review

- The school will monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied in practice.
- The policy framework will be reviewed at least annually, and in response to any new national guidance or legislation, significant developments in the use of technology, emerging threats or incidents that have taken place.

Useful sources of advice

- Teaching Online Safety in School (DfE)
- Education for a Connected World (UKCIS)
- Cyberbullying: understand, prevent and respond (Childnet)

- Cyberbullying: advice for Head Teachers and school staff (DfE)

Guided Home Learning

In the future, Guided Home Learning may well continue to be a managed part of the curriculum, either as ameans of providing support for individual pupils in specific circumstances, or as part of a more flexible and diverse educational offer which the school will continue to develop and enhance over time. Live online sessions must only take place through approved school platforms. One-to-one online meetings between staff and pupils should only occur where educationally necessary, be authorised by school leaders and follow safeguarding procedures. Where online sessions are recorded, storage and retention arrangements must comply with school data protection procedures.

Formats for Home Learning

There is a wide range of formats for guided home learning, including:

- Posting activities for pupils at regular intervals, with pupils posting responses.
- Providing recorded material in the form of podcasts or video tutorials.
- Directing pupils to web-based resources and activities they can engage with on or offline.
- Interactive/live teaching in real time.

Teachers will select the most appropriate format depending on a number of factors, including the age of thepupils, size of the group, nature of the activity, and the degree of support required; and taking into account

the need to provide a variety of learning experiences within a lesson, across the school day/week and through a scheme of work.

For staff:

- Only use school approved platforms; do not use social media in communicating with pupils.
- Keep a record/log of live online lessons – date and time, attendance, what was covered, any incidents.

o Maintain professional conduct during live streaming – dress appropriately, consider your surroundings (background, other household members who may come into view etc.) and blur if necessary, and rememberthat your microphone may be on.

o Maintain the same boundaries and insist on the same standard of behaviour as in a school setting and make specific protocols clear at the outset, e.g., muting of microphones at appropriate times, use of supervised chat only, etc.

For pupils:

- Be aware that some live online sessions may be recorded by the teacher.
- Dress appropriately for online lessons.
- Ensure that you have a safe and appropriate place to participate from. Blur your background if necessary.
- Follow the school rules for conduct during online lessons as if you were in school.

- Do not undermine in any way the technology used to offer video lessons.

- If you have concerns about online safety, or if you feel you are being bullied, talk to someone youtrust.

The role of parents

- It is the responsibility of parents to ensure that pupils are monitored in their use of technology for guided home learning as they would ordinarily do when their children are using technology at home.

- While students are working from home, they are connected to their home broadband so their traffic doesn't go through the school firewall – parents will therefore need to ensure that age appropriate filteringis enabled at home.

Being Responsible Digital Citizens

At Newton International Academy Smash we are committed to fostering a safe, respectful, and responsible online environment. As part of our digital learning community, all students, staff, and parents are expected to act as responsible digital citizens.

A responsible digital citizen at NIA Smash does the following:

1. **Using Artificial Intelligence Responsibly**

- Understands that AI-generated information may not always be accurate, unbiased or appropriate.
- Use AI tools ethically and responsibly, ensuring that schoolwork reflects their own understanding and effort.
- Recognise that AI must not be used to create harmful, offensive, discriminatory or inappropriate content.

2. **Respects Others Online**

- Communicates kindly and respectfully in all digital interactions.
- Avoids cyberbullying, harassment, or posting harmful or offensive content.
- Acknowledges others' opinions and engages in constructive discussions.

3. **Protects Personal Information**

- Understands the importance of keeping passwords, addresses, and other personal data private.
- Avoids sharing identifying information online without permission from a trusted adult.

4. **Uses Technology Responsibly**

- Uses devices, apps, and internet services for educational and appropriate purposes during school time.
- Does not engage in illegal downloading or access age-inappropriate content.
- Reports any unsafe or inappropriate online behavior or content to a trusted adult or staff member.

5. **Thinks Critically About Online Content**

- Understands that not everything online is true or trustworthy.
- Uses multiple sources to verify information and avoids spreading misinformation.

6. **Respects Intellectual Property**

- Credits all sources when using or referencing others' work, including text, images, and music.
- Understands the importance of copyright and plagiarism rules.

Teaching and Promoting Digital Citizenship:

All students receive regular instruction on digital citizenship as part of our computing and PSHE curriculum.

Staff model positive digital behavior and guide students in navigating the online world safely and ethically.

By promoting digital citizenship, we aim to empower our school community to use technology thoughtfully, respectfully, and safely—both in and outside the classroom.

As a British international school, NIA Smash promotes responsible, ethical and respectful use of technology. Through our curriculum and pastoral provision, pupils develop the knowledge, skills and values required to participate safely and positively in an increasingly digital and interconnected world.

The school promotes digital wellbeing, digital literacy, online resilience and responsible participation in local and global communities in line with CIS and BSO expectations.