NEXUS INTERNATIONAL SCHOOL (SINGAPORE)
REGISTRATION NO. 201009668C
1 ALJUNIED WALK, SINGAPORE 387293
T +65 6536 6566
www.nexus.edu.sg

RESPONSIBLE TECHNOLOGY USE GUIDELINES

PURPOSE

This document exists to outline a collective understanding of our philosophy and practical approaches to ensure that technology is used in ways that support learning and well-being and protect members of the School community. It is focused on upholding the values of community, relationships, respect, responsibility and integrity that underpin life at Nexus.

At Nexus, learners are provided with access to powerful digital tools that support inquiry, collaboration, creativity and deep learning. Technology is an important part of modern education and, when used thoughtfully, can significantly enhance the learning experience. The School works in partnership with families to promote the understanding that devices provided for learning should primarily be used for educational purposes while learners are on campus.

At the same time, digital technologies present challenges relating to wellbeing and distraction, therefore the development of positive online habits and behaviours is key to supporting learners to develop habits that will enhance their personal wellbeing.

These guidelines apply to all learners using school-provided or personal devices on the School site, while participating in school activities, or where online behaviour has a direct impact on the wellbeing of members of the School community or the reputation of the School.

DIGITAL MATURITY AND RESPONSIBLE TECHNOLOGY USE

Access to digital technology at Nexus is based on the expectation that learners develop digital maturity.

Digital maturity refers to the ability to use technology thoughtfully, responsibly and with clear purpose. It involves understanding that digital actions can have lasting consequences and that online behaviour should reflect the same standards of respect and responsibility expected in person.

Learners who demonstrate digital maturity:

- use technology with clear purpose to support learning and creativity
- understand the positive and negative consequences of use of technology and apply these in their daily life
- avoid behaviours that fragment attention or disrupt learning
- respect the dignity, privacy and digital identity of others
- think critically about the information they encounter online
- understand that digital content may remain publicly accessible and permanent
- act responsibly when using social media and other online platforms

- understand that some digital platforms are designed to capture attention and can contribute to harmful patterns of use, including dopamine-driven feedback cycles linked to notifications and "likes"
- use emerging technologies, including artificial intelligence, ethically and responsibly.

Developing digital maturity is an ongoing process. The School supports this through digital citizenship education, day-to-day learning, assemblies, workshops, and guidance from teachers and staff. Learners are expected to take increasing responsibility for their digital behaviour as they grow and mature.

KEY DEFINITIONS

Term	Definition
BYOD	Bring Your Own Device (BYOD) - A policy allowing staff or learners to use their personal devices (e.g., laptops, smartphones, tablets) to access the School's ICT systems and resources. Specific security measures must be followed for these devices.
Content Filtering	Technology used to restrict access to certain types of online content.
Cyberbullying	Involves bullying through digital platforms, such as social media, messaging apps, or online gaming.
Cybersecurity	Protection of ICT systems, networks, and data from unauthorised access, attacks or damage. It includes measures like firewalls, antivirus software, and encryption.

Term	Definition
Data Privacy	The protection of personal data, ensuring that it is collected, stored, and processed in compliance with laws such as the **Personal Data Protection Act (PDPA)**. It safeguards individuals' rights to control their personal information.
Digital Citizenship	The responsible and ethical participation in digital environments. Digital citizenship includes respecting others online, communicating appropriately on digital platforms, protecting personal and community wellbeing, and understanding the rights and responsibilities that accompany the use of digital technologies.
Digital Literacy	The ability to use digital technologies effectively to access, evaluate, create and communicate information. Digital literacy includes understanding how digital tools work, how to assess the reliability of online information, and how to use technology productively for learning, research and communication.
Digital Maturity	The ability to use digital technologies thoughtfully, responsibly and with sound judgement. Digital maturity involves managing device use appropriately, understanding the potential consequences of online behaviour, respecting privacy and digital identity, and making responsible choices when using digital platforms and emerging technologies. Digital maturity goes beyond technical skill and reflects the attitudes, habits and

	judgement required to participate safely and responsibly in digital environments.
Social Media Platform	Any online service that enables users to create, publish or interact with publicly or privately distributed content such as text, images, video or live streams. Examples include TikTok, Instagram, Snapchat, WeChat, Telegram, WhatsApp, YouTube, X (Twitter), Facebook and similar services.
Firewall	A security system that monitors and controls incoming and outgoing network traffic. It helps to prevent unauthorised access to or from a private network.
ICT	Information and Communication Technology.
Recreational Device Use	Use of a digital device for entertainment or non-educational purposes while on the School site. This includes activities such as gaming, social media browsing, entertainment streaming or extended non-academic messaging.
Filming or Recording	Capturing audio, images or video using any digital device, including mobile phones, tablets, smart watches, wearable cameras or similar technologies.
Artificial Intelligence (AI)	Computer systems designed to perform tasks that normally require human intelligence, such as generating text, images, analysing data or recognising patterns.
Generative Artificial Intelligence (GenAI)	A category of artificial intelligence tools capable of generating new content such as text, images, audio or video based on patterns learned from large datasets.
Agentic Artificial Intelligence (Agentic AI)	Artificial intelligence systems that can autonomously plan, make decisions, and carry out multi-step tasks in order to achieve a defined goal.
Phishing	A type of cyberattack in which fraudulent emails, messages, or websites are used to trick individuals into revealing sensitive information, such as passwords or credit card details.
Remote Access	The ability to access the School's ICT systems and resources from off-site locations, such as from home. Remote access must be secure and follow the same rules as on- site access, including encryption and password protection.
Safeguarding	Protection of individuals, especially children and vulnerable persons, from harm or abuse.
Virtual Private Network (VPN)	A secure method for connecting to a network over the internet. VPNs are often used to access School ICT resources remotely, encrypting the data to protect it from unauthorised access.
Digital Footprint	The collection of information and content that exists online about a person as a result of their digital activities, including posts, comments, images, videos and other shared data.
Cyberbullying	Bullying or harassment that occurs through digital technologies, including social media platforms, messaging applications, gaming environments or other online spaces.
Reputational Harm	Content or behaviour published online that damages the wellbeing of members of the School community or brings the School into disrepute.

ROLES AND RESPONSIBILITIES

Creating a safe and purposeful digital environment is a shared responsibility across the school community. A collective understanding of why we are encouraging technology to be used positively and how we ensure the safety and wellbeing of our community will enhance learning and help prepare our learner for life after Nexus. All members of the community have their part to play. More details of roles and responsibilities can be seen in Appendix F.

PURPOSEFUL USE OF DEVICES AT SCHOOL

Digital devices such as iPads and mobile phones are valuable learning tools when used appropriately. On the School site, devices should be used primarily to support learning activities and academic work.

At School, devices should only be used for learning-related purposes or when directed by a teacher.

Recreational use of devices is not permitted on the School site. This includes activities such as:

- playing games
- browsing or posting on social media platforms
- streaming entertainment content
- engaging in extended non-educational messaging.

Learners may occasionally need to use their phones briefly for practical purposes, such as arranging transport home. However, this does not extend to recreational device use while on campus.

Using devices purposefully helps maintain a focused learning environment and supports the wellbeing and attention of all learners.

Device Use Before School, During the School Day and After Lessons

Expectations regarding device use apply throughout the time that learners are on the School site.

Recreational use of phones or iPads is not permitted before School, during the School day, between lessons, or after lessons while on campus.

Learners are expected to use devices responsibly and in ways that support the learning environment at all times.

At the end of the School day, learners should leave campus promptly unless they are participating in a supervised activity such as a co-curricular activity, learning support session, or other organised programme.

The Learning Resource Hub and other supervised areas operate within specific hours. Outside of these structured activities, the School does not provide supervision for learners remaining on

campus after the end of the timetabled day.

Learners who remain on campus without participating in a supervised activity and who are found using devices for recreational purposes may have their device temporarily confiscated and returned at a later time determined by staff.

Parents and caregivers are encouraged to speak with their children about making clear plans for the end of the School day and leaving campus promptly unless they are involved in supervised activities.

Social Media Age Requirements and Reporting

Most major social media platforms require users to be at least 13 years of age in order to create an account.

Learners should comply with the age requirements and terms of service of the platforms they use.

Where the School becomes aware of accounts believed to belong to learners who are below the minimum age required by a platform, the School may report the account to the platform provider using the appropriate reporting channels.

The purpose of such reporting is to support the enforcement of platform safety standards and to help protect younger users from potential risks associated with social media use.

Parents and caregivers remain responsible for supervising their child's use of social media platforms outside of school. The School can provide guidance and support where families require assistance in reporting underage accounts.

Social Media Conduct

Online behaviour forms part of the expectations for respectful conduct within the Nexus community. Learners are expected to demonstrate the same standards of respect, responsibility and integrity online as they would in person.

- Learners must not create, publish or share online content that:
- targets, mocks or humiliates any member of the School community
- invites or amplifies negative judgments about members of the School community
- harms the wellbeing or dignity of another person
- misrepresents individuals or events within the School
- damages the reputation of the School or brings the School into disrepute.

Content published on public platforms can spread quickly and remain accessible indefinitely. Learners should carefully consider the potential impact of what they post or share online, particularly when content identifies the School, its learners or its staff.

Online behaviour that harms the wellbeing of members of the community or undermines the respectful culture of the School may result in disciplinary action in accordance with School's

policies and agreements.

Where content published online harms the wellbeing of members of the School community, targets staff or learners, or damages the reputation of the School, the School may take appropriate steps to address the situation.

This may include requesting that the content be removed, contacting the platform on which the material has been published, and following up with the learners involved to reinforce expectations regarding respectful and responsible digital conduct.

In cases where online behaviour significantly affects the wellbeing of members of the School community or the reputation of the School, the matter may be addressed in accordance with the Engagement and Behaviour Policy and Guidelines and the Student Contract and Terms and Conditions .

Artificial Intelligence and Emerging Technologies

Artificial intelligence tools are increasingly used in education and everyday life. When used appropriately, these technologies can support learning, research and creativity.

Learners are expected to use artificial intelligence tools responsibly and in accordance with the **Taylor's Schools Artificial Intelligence Policy**.

Learners must not use artificial intelligence or other digital technologies to:

- impersonate another person
- create manipulated or misleading media depicting real individuals
- generate harmful or inappropriate content about members of the School community
- submit AI generated work dishonestly or in a way that breaches the School's Academic Integrity Policy.

Cybersecurity and Network Integrity

Members of the School community share responsibility for maintaining the security and integrity of the School's digital systems.

Learners must not attempt to bypass, disable or interfere with the School's network security measures. This includes the use of tools designed to obscure network activity or circumvent filtering systems.

Examples of prohibited activity include:

- using VPNs, proxy services or other tools to bypass school filtering systems
- installing unauthorised software or applications on their learning devices
- attempting to access restricted systems or accounts
- sharing passwords or login credentials with others.
- using personal hotspots, tethering or similar methods to bypass the School's network,

filtering or monitoring systems

Learners should use strong passwords and keep their account credentials private. Any suspected security issues, phishing attempts or unusual digital activity should be reported to a teacher or the ICT department as soon as possible.

Protecting the security of school systems helps ensure a safe and reliable digital environment for everyone.

Partnerships with Families and Guardians

Developing responsible digital habits is most effective when schools and families work together.

The School supports families through communication, resources and workshops designed to help parents and caregivers understand the opportunities and challenges associated with digital technology.

Parents and caregivers are encouraged to:

- discuss responsible online behaviour with their children
- supervise the use of social media platforms where appropriate
- support healthy digital habits at home
- ensure that learners have clear arrangements for leaving campus at the end of the school day.

Through open communication and shared expectations, the School and families can work together to support learners in developing positive and responsible relationships with technology.

Consequences and Escalation

The intention of these responses is to reinforce expectations, support the development of digital maturity and maintain a constructive, respectful and focused learning environment. Where technology is used in ways that do not align with these guidelines, the School may take appropriate steps to address the situation.

Responses may include:

- temporary confiscation of devices
- follow-up conversations with tutors or school leaders
- communication with parents or caregivers
- requests for inappropriate online content to be removed
- reporting underage social media accounts to platform providers where appropriate.
- In more serious cases, incidents may be addressed in accordance with the NISS Engagement and Behaviour Policy and Guidelines, NISS Safeguarding Policy and Student Contract and Terms and Conditions.

NEXUS INTERNATIONAL SCHOOL (SINGAPORE)
REGISTRATION NO. 201009668C
1 ALJUNIED WALK, SINGAPORE 387293
T +65 6536 6566
www.nexus.edu.sg

SUPPORTING POLICIES/GUIDELINES/HANDBOOKS

These guidelines should be read in conjunction with:

NISS Student Contract and Terms and Conditions
NISS Engagement and Behaviour Policy and Guidelines
NISS Safeguarding Policy
TSO ICT Acceptable Use and e-Safety Policy
TSO Artificial Intelligence (AI) Policy

REVIEW AND REVISION

These guidelines will be reviewed once every two (02) years or as required to reflect updates to the relevant legislations, Taylor's Schools group policies or internal school governance standards where applicable.

APPENDICES

Please refer to the Schools' specific documents (where applicable, if any):

- Schools' AUP - Staff and Learners templates
- Schools' Approved tools and platforms used for educational purposes
- Schools' Academic Integrity Policy
- Incident Report Form
- Taylor's Schools AI Policy
- Taylor's Schools ICT Acceptable Use and e-Safety Guidelines

These policies can be accessed via ParentZone or provided upon request.

Appendix A

Digital Wellbeing and Attention

Digital technologies can be powerful tools for learning, but excessive or unfocused device use can negatively affect attention, wellbeing and sleep.

Many digital platforms are designed to capture attention through rapid notifications, social feedback and continuous content streams. These features can encourage frequent checking behaviours and reduce the ability to focus for sustained periods.

Learners are encouraged to use technology purposefully rather than passively. This means prioritising activities such as research, creation, collaboration and learning over passive scrolling or entertainment.

Developing healthy digital habits is an important part of digital maturity. Learners are encouraged to maintain balance between digital activities and other aspects of school life, including reading, physical activity, creative pursuits and face-to-face interaction.

Through assemblies, lessons and workshops, the School supports learners in developing habits that promote focus, wellbeing and thoughtful technology use.

Appendix B

Digital Likeness, Consent and Deepfake Technologies

The School affirms that every individual has the right to control their own face, voice, and body in digital spaces. The creation, use, possession, or distribution of AI-generated or manipulated media, including deepfakes, that depict or imitate a real person without clear and informed consent is prohibited. Such practices undermine dignity, privacy, safety, and trust, and may constitute harassment or impersonation. Learners and staff are expected to use emerging

technologies responsibly and ethically, respecting the digital identity and likeness of others at all times. The School is committed to educating its community about digital identity, deepfake risks, and AI ethics.

Learners should recognise that emerging technologies require thoughtful and responsible use and should seek guidance from teachers when unsure about appropriate use.

Appendix C

Filming, Recording and Public Content

Respect for privacy and consent is an important part of responsible technology use.

Learners must not film, photograph or record staff or other learners on the School site without permission. This includes the creation of video content intended for social media platforms.

Learners must not:

- record audio or video of teachers or classmates without their consent
- create interviews, rankings or similar content involving members of the School community without permission
- livestream from the School site
- publish video content filmed on School premises or in school uniform without authorisation.

These expectations apply regardless of whether the recording device is a phone, tablet, wearable device or other digital technology.

Unauthorised recording or publication of content can undermine privacy, safeguarding and trust within the School community and will be treated as a serious breach of these guidelines.

Appendix D

Monitoring and Investigation

To help maintain a safe digital environment, the School may monitor activity on its networks and digital platforms.

Internet usage on the School network may be logged and reviewed in order to identify security risks, inappropriate activity or breaches of these guidelines. Monitoring is carried out in a manner that respects privacy while supporting safeguarding and responsible technology use.

Where concerns arise, the School may investigate digital activity that appears to breach School's

expectations or pose a risk to members of the community.

This may include reviewing network logs, speaking with the learners involved, and requesting that harmful or inappropriate online content be removed where it affects members of the School community or the reputation of the School.

Appendix E

Device Confiscation and Follow Up

Where devices are used in ways that do not comply with these guidelines, staff may temporarily confiscate the device.

Confiscated devices will normally be passed to Learner Services and returned to the learner at a later time determined by the School's Senior Leadership Team.

In such cases, learners may be asked to complete a short reflection and speak with their Tutor or Homeroom Teacher to reinforce expectations around responsible technology use.

These procedures are intended to support the development of digital maturity and to maintain a focused and respectful learning environment.

Appendix F

Roles & Responsibilities

Principal

The Principal provides overall leadership for the implementation of these guidelines, driving the whole school philosophy and approaches and ensuring that expectations relating to responsible technology use are applied consistently across the School.

Oversee the annual professional development programme for teachers on digital literacy, cybersecurity, and e-safety, while providing the necessary resources and support to facilitate this training and ongoing professional development for staff.

Addresses serious incidents involving harm to learners or staff in line with safeguarding protocols.

Facilitates access to counselling and mental health resources for victims and perpetrators of cyberbullying.

NEXUS INTERNATIONAL SCHOOL (SINGAPORE)
REGISTRATION NO. 201009668C
1 ALJUNIED WALK, SINGAPORE 387293
T +65 6536 6566
www.nexus.edu.sg

Director of Digital Learning & Entrepreneurship

The Director of Digital Learning & Entrepreneurship supports the Principal with providing strategic leadership in the responsible use of digital technologies. This includes supporting the development of digital maturity among learners, advising on emerging technologies, promoting digital wellbeing, and ensuring alignment with the Taylor's Schools Artificial Intelligence Policy.

IT & Infrastructure Department

Implements cybersecurity measures, including content filtering, anti-virus systems, and access controls.

Report the use of social media accounts by learners under the age of 13

Requests the deletion of social media accounts being used by learners under the age of 13 to said providers Keeps abreast of emerging technologies and updates security protocols accordingly.

Collaborate with the School's leadership to host digital safety workshops for parents, offering advice and resources on how to guide their children in safe online behaviour

Teachers and Staff

Demonstrate responsible and effective use of technology to inspire learners.

Report the use of social media accounts by learners under the age of 13

Ensure the safe and appropriate use of technology in the classroom and at work, reporting any policy breaches to the appropriate school leader.

Deliver programmes that support digital citizenship, cybersecurity, and healthy digital habits to foster a safe online environment and ensure the guidelines within this policy are adhered to

Engage in training opportunities focused on safe use of IT and that promote safe digital practices.

Actively identify and address online risks in the classroom while providing guidance and support to learners on their online behaviour and safety.

Teachers and staff have a professional responsibility to report concerns relating to online behaviour, inappropriate content, safeguarding risks or unsafe technology use in accordance with the School's Safeguarding Policy and reporting procedures.

Learners

Must use technology responsibly, adhering to the School's rules on internet use, mobile devices, and social media.

Reports the use of social media accounts by learners under the age of 13

Must report any exposure to inappropriate content or incidents to a teacher or designated staff member.

Engage in digital literacy programs and follow guidelines for safe online behaviour.

Must not use VPNs, proxy servers, or any other tools designed to obscure network traffic or bypass school filtering, monitoring, or security systems. Use of such tools undermines safeguarding measures and will be treated as a serious breach of this policy.

Learners should speak to a trusted adult or member of staff if they become aware of online behaviour, content or technology use that may place someone's wellbeing, safety or privacy at risk.

Parents

Play a key role in monitoring and guiding their children's technology use outside of school.

Reports the use of social media accounts by learners under the age of 13

Engage in conversations with their children about the importance of online safety and responsible digital citizenship.

Support the School's efforts by familiarising themselves with this policy and enforcing similar standards at home.