



Online Safety Protocol

Supporting Every Learner.
Empowering Every Potential.



SUPPORT



EQUITY



GROWTH



WELL-BEING



Middle States
Association



PINEWOOD AMERICAN INTERNATIONAL SCHOOL

1

Online Safety Protocol

Purpose and Scope	2
Online Safety key terms	3
Student Rights and Responsibilities	4
Online Safety Risks	4
School Response Procedures	10
Parent and Guardian Partnership	10
Review and Continuous Improvement	10
Digital Wellbeing and Healthy Technology Use	11
Appendix	12



Middle States
Association



PINEWOOD AMERICAN INTERNATIONAL SCHOOL

2

Purpose and Scope

Pinewood School is committed to providing a safe, respectful, inclusive, and supportive learning environment in both physical and digital spaces. The purpose of this Protocol is to promote the safe, responsible, ethical, and age-appropriate use of technology by students while protecting members of the school community from online risks and harm.

This Protocol establishes expectations, procedures, and responsibilities relating to online safety and digital conduct for students from Pre-Kindergarten all the way through Grade 12. It provides a framework for prevention, education, intervention, protection, and restoration in response to online safety concerns. Pinewood School recognizes that technology and digital communication are integral to modern learning, creativity, collaboration, and social interaction. Accordingly, this Protocol seeks to empower students to become informed, responsible, and resilient digital citizens who can engage safely and positively in online environments.

This Protocol applies to all students enrolled at Pinewood School, regardless of age or grade level.

The Policy applies to:

- School-owned devices, systems, networks, applications, and digital platforms
- Personal devices used on school premises or during school activities
- Digital interactions occurring within school-related activities, programs, virtual learning environments, or involving members of the school community.

***Important Note:** Online conduct occurring outside school hours and beyond the School's supervision, systems, or platforms remains the primary responsibility of parents and guardians; where such conduct significantly affects the safety, wellbeing, or educational experience of a student, Pinewood School may provide appropriate support, guidance, safeguarding assistance, and educational interventions, while not assuming responsibility for investigating, regulating, or resolving matters that fall outside its authority or legal jurisdiction.

Pinewood's Acceptable Use Policy can be found on our website [HERE](#).



Middle States
Association



PINEWOOD AMERICAN INTERNATIONAL SCHOOL

3

Online Safety key terms

For the purposes of this Protocol, the following definitions are provided to ensure a common understanding and consistent interpretation of key terms used. These definitions are intended to support the effective implementation of the Protocol.

Online Safety: The protection of students from physical, emotional, psychological, social, financial, sexual, reputational, or educational harm that may arise through the use of digital technologies and online environments.

Digital Citizenship: The responsible, ethical, respectful, and safe use of technology and participation in digital environments.

Cyberbullying: The use of digital technologies to harass, threaten, intimidate, humiliate, exclude, impersonate, or otherwise harm another person.

Personal Information: Any information that identifies or could reasonably identify an individual, including names, photographs, contact information, addresses, locations, account information, identification numbers, or other identifying details.

Grooming: A process through which an individual establishes trust or emotional connection with a child or young person for the purpose of manipulation, exploitation, abuse, or harm.

Doxxing: The publication, disclosure, or sharing of personal or identifying information without consent.

Sextortion: The use of threats, coercion, manipulation, or blackmail involving intimate images, videos, or personal information.

Artificial Intelligence (AI): Computer systems capable of generating, modifying, analyzing, or manipulating text, images, audio, video, or other forms of digital content.

Deepfake: AI-generated or digitally manipulated content designed to convincingly imitate a real person's appearance, voice, actions, or communications.

Digital Footprint: The lasting record of an individual's online activities, communications, content, and interactions.



Middle States
Association



PINEWOOD AMERICAN INTERNATIONAL SCHOOL

4

Harmful Content: Content that may be violent, hateful, discriminatory, sexually explicit, exploitative, self-harm related, extremist, misleading, or otherwise inappropriate for children and young people.

Student Rights and Responsibilities

Student Rights

Students have the right to:

- Learn in a safe and supportive digital environment.
- Be treated with dignity and respect in online interactions.
- Access age-appropriate online learning opportunities.
- Report online safety concerns without fear of retaliation.
- Receive support when affected by online harm or digital safety incidents.
- Have concerns addressed fairly, sensitively, and appropriately.
- Receive education that promotes safe and responsible technology use.

Student Responsibilities

Students are expected to:

- Use technology safely, responsibly, respectfully, and ethically.
- Respect the rights, privacy, dignity, and wellbeing of others.
- Protect personal information and account credentials.
- Abide to school technology, acceptable use, safeguarding, and behaviour expectations, that display integrity and good judgment in regards to digital content. Refer to the Academic Integrity Policy [HERE](#).
- Seek assistance when encountering online risks or concerns.
- Report harmful, unsafe, or inappropriate online behaviour.
- Refrain from engaging in conduct that may cause harm to themselves or others, and instead contribute positively to the online community.



Middle States
Association



PINEWOOD AMERICAN INTERNATIONAL SCHOOL

5

Online Safety Risks

The following categories identify online safety concerns that may affect children and young people. These examples are not exhaustive, and the School reserves the right to address emerging technologies, platforms, behaviours, and risks as they arise. Pinewood School is committed to educating students about these risks, implementing preventative measures, and responding appropriately to concerns.

1. Cyberbullying, Harassment, and Digital Abuse

Students may experience or engage in cyberbullying, online harassment, intimidation, humiliation, exclusion, threats, hate speech, discriminatory conduct, impersonation, or repeated harmful behaviour through digital technologies.

Such conduct may occur through social media platforms, messaging applications, gaming environments, email, collaborative learning platforms, discussion forums, livestreaming services, or anonymous communication tools.

2. Artificial Intelligence (AI), Deepfakes, and Manipulated Content

Artificial intelligence technologies increasingly enable the creation of realistic text, images, audio recordings, videos, conversations, and other forms of digital content. Students may be exposed to or engage in the creation, modification, or sharing of AI-generated or manipulated content, including deepfakes and synthetic media, aiming to deceive, manipulate, harass, bully, and generally harm the wellbeing of others.

3. Online Grooming, Exploitation, sextortion and image-based abuse

Students may be targeted by individuals seeking to establish trust or emotional connections through online games and social media platforms, or other digital environments. Such interactions may progress to manipulation, coercion, exploitation, requests for personal information, requests for photographs or videos, financial abuse, or sexual exploitation. Students should never feel pressured to share personal information, images, passwords, locations, or private communications with individuals they know only online.

4. Privacy Violations, Doxxing, and Unauthorized Disclosure



Middle States
Association



PINEWOOD AMERICAN INTERNATIONAL SCHOOL

6

Students have the right to privacy and the protection of personal information. The sharing, publication, or dissemination of personal information, photographs, addresses, contact details, location information, schedules, account credentials, or other identifying information without consent may place individuals at risk of harassment, intimidation, exploitation, identity theft, or physical harm.

Students should understand that online actions may create a lasting digital footprint. Content shared online may remain accessible, searchable, reproducible, and influential long after it is posted, regardless of whether it is later deleted.

Students should refrain from capturing or sharing content involving others and are expected to respect the privacy and dignity of all members of the school community.

5. Financial Exploitation, Fraud, and Online Scams

Students may be exposed to fraudulent schemes designed to obtain money, personal information, account credentials, financial information, or digital assets.

Examples may include phishing attacks, cryptocurrency scams, fake competitions, fraudulent marketplaces, impersonation scams, investment schemes, gaming-related fraud, and deceptive online advertisements.

Students should exercise caution when interacting with requests involving money, passwords, account access, personal information, or financial transactions.

6. Harmful Online Influential trends

Students may encounter online challenges, dares, trends, or social media movements that encourage risky, dangerous, unlawful, self-destructive, exploitative, or harmful behaviour. Participation in such activities may result in physical injury, emotional harm, reputational damage, legal consequences, or risks to others. Students are encouraged to critically evaluate online trends and seek guidance when uncertain about the safety or appropriateness of online content.

Online Radicalization and Extremist Influence: Individuals or groups may use digital platforms to promote extremist ideologies, hateful beliefs, violence, discrimination, or harmful activities.



Middle States
Association



PINEWOOD AMERICAN INTERNATIONAL SCHOOL

7

7. Livestreaming and Video-Sharing Risks

Livestreaming platforms and video-sharing services may expose students to inappropriate contact, harassment, exploitation, privacy violations, public humiliation, or pressure to engage in risky behaviour before an audience.

Students should understand that livestreamed content may be recorded, copied, redistributed, or permanently archived regardless of platform settings.

Pinewood School encourages students to exercise caution when broadcasting personal information, locations, activities, or images online.

8. Exposure to Harmful or Inappropriate Content

Students may encounter content that is violent, sexually explicit, discriminatory, hateful, exploitative, graphic, self-harm related, age-inappropriate, or otherwise harmful to their wellbeing. Additionally, there are certain applications that provide encrypted communication, disappearing messages, temporary content, anonymous communication, or limited oversight.

Exposure may occur intentionally or unintentionally through websites, social media platforms, advertisements, search results, recommendation algorithms, messaging applications, gaming environments, or peer sharing.

9. Data Security and Account Protection

Students are expected to take reasonable steps to protect their accounts, passwords, devices, and personal information. Sharing passwords, circumventing security measures, accessing accounts without authorization, attempting to compromise systems, or engaging in activities that threaten digital security is prohibited.

Reporting Process

Pinewood School encourages the timely reporting of all online safety concerns, incidents, risks, or suspected violations of this Protocol.

Students, parents, guardians, staff members, volunteers, and visitors share responsibility for helping to maintain a safe digital environment and are encouraged to report concerns whenever they arise.



Middle States
Association



PINEWOOD AMERICAN INTERNATIONAL SCHOOL

8

Pinewood School recognizes that reporting online safety concerns may be difficult or uncomfortable. Reports will be taken seriously, treated with sensitivity, and addressed in a manner that prioritizes student safety and wellbeing.

All the aforementioned concerns of online safety taking place in school need to be reported and addressed. Students are encouraged to report concerns even when they are uncertain whether a particular situation constitutes a policy violation.

1. Reporting Pathways

Students and parents/ guardians may report concerns to:

- Faculty and staff
- School psychologist/ Child Protection Officer
- A member of the safeguarding or student support team
- Principals

Staff members who receive reports or become aware of online safety concerns are expected to follow the procedures outlined below.

2. Preserving Evidence

Students, parents, guardians, and staff should avoid deleting potentially important evidence before it has been reviewed. Where safe and appropriate, individuals may be encouraged to preserve:

- Screenshots/ Messages/ Emails/ Usernames
- Website addresses
- Images/ Videos
- Dates and times of incidents
- Other relevant documentation.

Preservation of evidence may assist in investigation, safeguarding assessments, restorative processes, disciplinary decisions, or referrals to external authorities.

3. Confidentiality and Information Sharing

As per Pinewood's Child Protection and Safeguarding Policy:
Confidentiality



Middle States
Association



PINEWOOD AMERICAN INTERNATIONAL SCHOOL

9

Pinewood respects the privacy of those involved in all aspects of child protection cases. Safeguarding records will be retained securely in accordance with applicable Greek law, GDPR requirements, and the school's data retention policy. Access will be restricted to authorized personnel only.

However, those involved must understand that in order for an inquiry into the incident to proceed, certain information must be shared. Information will be shared strictly on a need-to-know basis and only with those directly involved in incident response. These individuals may include but are not limited to the Child Protection Team, Pinewood leadership, Board of Trustees, and/or Greek child protection officials.

Information Sharing

Pinewood policy regarding confidentiality and management of school records applies to all record keeping and documentation of incidents of child protection. Only designated faculty and staff, such as the school counselor and the school nurse or the Child Protection Officer have access to confidential documentation regarding child protection matters.

Employees should never use or disclose confidential or personal information about a student or their family, in casual conversations or other context, since this information might be used by other parties to humiliate or embarrass a student.

In case an abuse is alleged or suspected, then employees have the responsibility to break confidentiality and inform the designated person without delay. If a child or parents make a disclosure regarding abuse, the member of the staff should not promise confidentiality, but give reassurance that the information will be treated in a sensitive and effective manner. In case of doubts, please contact the school counselor or the child protection officer.

All parties involved in the reporting and intervention procedure should sign the [Confidentiality Agreement](#).

4. Protection from Retaliation

No student, parent, guardian, or staff member shall be subjected to retaliation for making a good-faith report of an online safety concern. Any attempt to intimidate, threaten, harass, or retaliate against an individual who reports a concern constitutes a violation of Pinewood's expectations and values.



Middle States
Association



PINEWOOD AMERICAN INTERNATIONAL SCHOOL

10

School Response Procedures

Pinewood School is committed to responding promptly, fairly, proportionately, and consistently to online safety concerns. Refer to the [Child Protection and Safeguarding Handbook](#) for the responding steps and the record keeping.

Parent and Guardian Partnership

Pinewood School recognizes that parents and guardians play a vital role in promoting online safety and responsible technology use.

Effective online safety education is strengthened through ongoing collaboration between home and school.

Parents and guardians are encouraged to:

- Promote safe and responsible technology use at home
- Maintain open and age-appropriate conversations about online experiences
- Support healthy digital habits and digital wellbeing
- Monitor and guide technology use in a manner appropriate to the age and maturity of their child
- Familiarize themselves with emerging technologies, applications, and online risks
- Encourage prompt reporting of online safety concerns
- Collaborate with the School when concerns arise.

Pinewood School is committed to supporting families through communication, education, guidance, and partnership in matters relating to student online safety.

Review and Continuous Improvement

Pinewood School recognizes that technology, digital environments, and online risks continue to evolve.



Middle States
Association



PINEWOOD AMERICAN INTERNATIONAL SCHOOL

11

This Protocol shall be reviewed periodically to ensure its continued effectiveness, relevance, and alignment with current best practices, safeguarding requirements, legal obligations, and emerging technologies.

Pinewood School may update procedures, guidance, educational initiatives, and response practices as necessary to address new developments and identified needs.

Feedback from students, parents, guardians, staff members, and other stakeholders may inform future revisions and improvements.

Through ongoing review, education, and collaboration, Pinewood School seeks to maintain a proactive, preventative, protective, and restorative approach to online safety that supports the wellbeing and success of all students.

Digital Wellbeing and Healthy Technology Use

Pinewood School recognizes that excessive or unhealthy use of digital technologies may affect students' physical health, sleep, academic performance, relationships, emotional wellbeing, and overall development.

Students are encouraged to develop balanced technology habits, healthy boundaries, self-regulation skills, and positive online behaviours.

Digital wellbeing education may include topics such as screen time balance, sleep hygiene, online relationships, emotional resilience, self-image, social comparison, and responsible technology use.



Middle States
Association

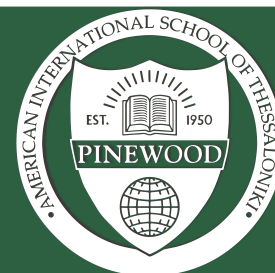


PINEWOOD AMERICAN INTERNATIONAL SCHOOL

12

Appendix

Recognizing and Responding to Online Safety Concerns



Concern Identified	A student, parent, guardian, staff member, or community member identifies a potential online safety concern, risk, or incident.
Report	The concern is reported to an appropriate staff member, counsellor, safeguarding lead, or administrator.
Assessment	The School evaluates the nature of the concern, identifies any immediate risks, and determines whether safeguarding action is required.
Support & Safeguarding	Immediate steps are taken to protect student safety, wellbeing, and access to appropriate support.
Investigation	Relevant information is gathered and reviewed to understand the circumstances and determine appropriate next steps.
Educational / Restorative / Disciplinary Response	The School implements one or more responses, which may include: • Educational interventions • Restorative or reparative measures • Supportive wellbeing measures • Disciplinary action where necessary
Follow-Up & Monitoring	Pinewood School monitors student wellbeing, reviews outcomes, and provides ongoing support as needed.
Review & Continuous Improvement	Pinewood School evaluates practices, identifies lessons learned, and updates procedures, education, and prevention efforts where appropriate.