



Digital Usage Policy

Introduction:

At DPS, RAK, we recognize that digital technologies are essential to learning, communication, creativity, collaboration, and everyday school life. We believe every student has the right to use technology safely, responsibly, respectfully, and purposefully. We are committed to creating a digitally responsible environment in which technology enhances learning without compromising safeguarding, privacy, wellbeing, academic integrity, or the rights of others.

We actively promote digital citizenship and have clear expectations and procedures for the responsible use of school and personal devices, online platforms, social media, digital communication, and Artificial Intelligence (AI).

Aims and Objectives:

- At DPS RAK, we promote safe, responsible, respectful, and purposeful use of digital technologies by all members of the school community.
- We are committed to protecting students and staff from online harm, inappropriate content, cyberbullying, privacy breaches, scams, misuse of technology, and other digital safeguarding risks.
- We aim to develop students' digital literacy, critical thinking, media literacy, information literacy, and ability to make responsible decisions online.
- We expect all users to respect others' privacy, intellectual property, dignity, wellbeing, and digital rights.
- We recognise that Students of Determination may require additional support, reasonable adjustments, and explicit teaching to access and use digital technologies safely.
- We promote responsible and transparent use of Artificial Intelligence, ensuring that AI supports learning and does not replace students' thinking, creativity, effort, or accountability.
- All stakeholders, including students, staff, parents, and the wider school community, share responsibility for responsible digital use.

Purpose and Scope

The school's aim for Student Welfare is to meet each individual's personal, educational, and social needs in a healthy, safe, and secure environment. Digital technologies should contribute positively to this environment and support learning, communication, collaboration, creativity, and student wellbeing.

This policy applies to all students and covers school-owned devices; personally owned devices used in connection with school; school networks and internet access; learning platforms; email; messaging applications; social media; online meetings; digital resources; cloud services; gaming where it affects school life; and Artificial Intelligence tools.

The policy applies on school premises, during school transport, educational visits, residential activities, competitions, clubs, events, online learning, remote learning, and any other context where digital behaviour may affect the safety or wellbeing of the DPS community.

Digital usage must comply with school rules, safeguarding procedures, applicable UAE laws and regulatory requirements, and the terms and conditions of approved digital platforms. The school may restrict or withdraw access to digital systems where use is unsafe, inappropriate, unlawful, disruptive, or inconsistent with this policy.

Digital Usage Expectations:

All students are expected to:

- Use digital devices and platforms for learning and other authorised purposes.
- Follow teachers' instructions regarding when, where, and how devices may be used.
- Keep usernames, passwords, authentication information, and personal security details private.
- Use strong passwords and follow school guidance for account security.
- Respect the privacy and dignity of others and never access, record, photograph, screenshot, share, or publish another person's information or image without appropriate permission.
- Communicate online using language and behaviour that demonstrate the same respect expected in face-to-face interactions.
- Use only approved or authorised accounts, platforms, applications, websites, and digital resources where required by the school.
- Check the reliability and credibility of information before using or sharing it.
- Respect copyright, licensing, ownership, and intellectual property.
- Report unsafe, inappropriate, harmful, suspicious, or concerning digital content or behaviour to a trusted adult.

Prohibited Digital Behaviour:

- Cyberbullying, harassment, intimidation, threats, humiliation, discrimination, or deliberate exclusion through digital platforms.
- Accessing, creating, storing, sharing, downloading, or distributing inappropriate, offensive, harmful, illegal, or age-inappropriate content.
- Attempting to bypass school filtering, security controls, monitoring systems, passwords, access restrictions, or network safeguards.
- Using another person's account, identity, password, device, or digital information without permission.
- Recording, photographing, filming, screenshotting, livestreaming, or distributing images/audio/video of students, staff, or visitors without appropriate permission.
- Creating or sharing fake accounts, impersonating another person, or using digital tools to deceive, threaten, embarrass, or harm others.
- Using digital technology to cheat, plagiarise, fabricate work, or misrepresent another person's work as one's own.
- Using school technology or online platforms for unauthorised commercial activity, inappropriate gaming, gambling, or other activities that conflict with school expectations.
- Installing or using unauthorised software, applications, extensions, scripts, or other tools that compromise security or interfere with school systems.
- Sharing personal, confidential, sensitive, or identifying information about another person without appropriate authorisation.

Personal Devices and Mobile Phones:

- Personal devices may only be used during the school day in accordance with the school's instructions and approved routines.
- Students must follow classroom and school-wide expectations regarding mobile phones, smartwatches, tablets, laptops, earbuds, and other connected devices. **At DPS, students should not bring mobile phones or wear smartwatches or earbuds.**
- Devices must not be used to disrupt lessons, record others, access inappropriate content, or facilitate unauthorised communication.

- Where a device is required for learning, students must use it for the stated educational purpose and follow teacher directions.
- The school is not responsible for loss or damage to personal devices brought to school, except where responsibility is established under applicable procedures.

Digital Wellbeing:

- Students should maintain a healthy balance between screen-based activities, physical activity, sleep, face-to-face relationships, and other aspects of wellbeing.
- Students should use respectful online communication and seek help if digital interactions cause distress, anxiety, intimidation, or harm.
- Teachers may establish screen-free or device-free periods to support attention, discussion, practical learning, physical activity, and wellbeing.
- Students should report harmful online content or behaviour rather than retaliating or further distributing it.

Recommendations for Students:

If you experience a digital safety concern:

- STOP – Do not respond impulsively to threatening, harmful, or inappropriate messages.
- SAVE – Where appropriate and safe, preserve relevant evidence such as messages, links, or screenshots. Do not circulate the material further.
- BLOCK – Use appropriate platform controls to block or restrict the person responsible where safe to do so.
- TALK – Tell a trusted adult, class teacher, Head of Phase, School Counsellor, Designated Safeguarding Lead, or another member of staff.
- REPORT – Use the school's reporting route or the platform's reporting tools for inappropriate or harmful content.
- SEEK HELP – If you or someone else is at immediate risk, seek adult help immediately.

If you witness online bullying or unsafe digital behaviour:

- Do not join in, like, share, forward, comment on, or encourage harmful content.
- Do not spread rumours, screenshots, recordings, or messages that may increase the harm.
- Support the person affected and encourage them to speak to a trusted adult.
- Report the concern promptly to an appropriate staff member.
- Do not confront or threaten the person responsible.

Procedure for Teachers/School Administrators to Deal with Digital Concerns:

- All reports of cyberbullying, inappropriate digital behaviour, privacy concerns, harmful content, account misuse, or other digital safeguarding concerns must be treated seriously.
- The staff member receiving the concern must ensure immediate safety and report the matter through the appropriate safeguarding, pastoral, disciplinary, or IT channel.
- Where a concern involves a student's safety or wellbeing, the Designated Safeguarding Lead/School Counsellor and relevant Head of Phase will be informed as appropriate.
- Staff must preserve relevant evidence where necessary and must not forward inappropriate content unnecessarily.
- Investigations will be conducted proportionately, sensitively, and in accordance with school procedures and applicable requirements.

- The school will confiscate gadgets if students install games on devices used at school after the first verbal warning. The school will return confiscated gadgets only by the end of the academic year, depending on the severity of the matter and violation, as stipulated in the parent contract.
- Parents/guardians will be informed where appropriate and in accordance with safeguarding considerations.
- The school will provide appropriate support to students affected by online harm and will monitor the situation until the concern has been addressed.
- The school will escalate serious or potentially unlawful incidents to senior leadership and relevant external or regulatory authorities where required.

Parents' Role in Supporting Safe Digital Usage

- Talk regularly with children about online safety, respectful communication, privacy, cyberbullying, misinformation, scams, and responsible technology use.
- Encourage children to tell a trusted adult when they encounter inappropriate, frightening, threatening, or harmful online content.
- Support age-appropriate boundaries around devices, applications, social media, gaming, and screen time.
- Help children use privacy settings, strong passwords, and appropriate account security.
- Monitor online activity appropriately while maintaining open communication and trust.
- Do not forward or circulate harmful images, messages, recordings, or rumours involving students or staff.
- Work collaboratively with the school when a digital safeguarding concern arises.
- Support the school's expectations regarding devices and digital learning.

Artificial Intelligence (AI) Usage

DPS RAK recognises that Artificial Intelligence can support learning, creativity, accessibility, research, planning, feedback, and problem-solving. AI must be used as a learning support, not a substitute for independent thinking, professional judgement, creativity, or responsibility. The school promotes responsible, transparent, age-appropriate, and ethical AI use.

AI Expectations for Students:

- Use only AI tools that are authorised or permitted, and which are appropriate for the student's age and learning context.
- Follow the teacher's instructions about whether and how AI may be used for a particular task.
- Do not submit AI-generated work as entirely your own when the task requires independent work.
- Acknowledge or disclose AI assistance when required by the teacher or assessment instructions.
- Use AI to support brainstorming, questioning, explanation, revision, feedback, language support, or other permitted learning purposes rather than to avoid learning.
- Check AI-generated information for accuracy, relevance, bias, and reliability before using it.
- Do not assume that an AI-generated answer is correct simply because it is confidently presented.
- Do not enter personal, confidential, sensitive, identifying, or private information about yourself or another person into an AI tool unless specifically authorised and appropriately protected.
- Do not use AI to create harmful, deceptive, discriminatory, threatening, sexual, humiliating, or misleading content.
- Do not use AI to impersonate another person, create fake evidence, manipulate images or recordings deceptively, or damage another person's reputation.
- Do not use AI to bypass assessment conditions, generate answers during restricted assessments, or otherwise gain an unfair academic advantage.

AI and Academic Integrity:

- Students remain responsible for the accuracy, originality, quality, and integrity of work they submit.
- Where AI use is permitted, students must be able to explain their ideas, decisions, sources, and contribution to the work.
- AI-generated text, images, code, translations, or other outputs must not be presented as independently produced work when this would breach assessment instructions.
- Students must respect copyright and intellectual property when using AI-generated or AI-assisted content.
- Teachers may use appropriate questioning, drafting processes, oral discussion, version history, or other evidence of learning to establish student understanding where necessary.

AI Expectations for Staff:

- Use AI tools professionally, ethically, and in accordance with school-approved systems and procedures.
- Do not enter confidential student, staff, parent, safeguarding, assessment, medical, or other sensitive information into public AI systems unless the system has been approved for that purpose and appropriate safeguards are in place.
- Verify AI-generated information before using it in teaching, assessment, communication, or decision-making.
- Do not rely solely on AI for safeguarding, disciplinary, admissions, grading, or other high-impact decisions.
- Ensure that AI use supports inclusion, accessibility, creativity, critical thinking, and professional judgement.
- Inform students when AI has been used in a way that materially affects learning resources or communications where transparency is appropriate.

AI and Privacy, Safeguarding and Digital Citizenship:

- Students and staff must protect personal and confidential information when using AI.
- AI must not be used to create or distribute harmful deepfakes, manipulated images, impersonations, or deceptive content involving members of the school community.
- Report any suspected misuse of AI involving bullying, safeguarding, privacy, impersonation, fraud, or harmful content promptly.
- The school will provide age-appropriate education about AI limitations, bias, misinformation, privacy, copyright, and responsible use.

Digital Learning Platforms and Online Classes

- Students must use school learning platforms, Teams, email, and other approved systems respectfully and for authorised purposes.
- Students must not remove, edit, damage, delete, or interfere with digital resources belonging to teachers or other students without permission.
- Students must not mute, remove, impersonate, or disrupt participants in an online class without teacher authorisation.
- Abusive language, inappropriate chat, unwanted content, unauthorised recording, and disruptive behaviour are prohibited.
- Students must use their assigned accounts and must not share login credentials.
- Teachers may establish additional expectations for individual online lessons or digital activities.

Information, Research and Media Literacy

- Students should use credible and age-appropriate sources when researching.
- Students should compare information from more than one reliable source where appropriate.
- Students should identify advertising, opinion, misinformation, manipulated content, and unreliable sources.

- Students must acknowledge sources and avoid plagiarism.
- AI-generated information must be independently checked before it is relied upon.

Formal Procedures in Response to an Incident of Digital Misuse

- Each step under this procedure should be undertaken without unreasonable delay, and careful records must be kept and filed appropriately.
- The relevant Head of Phase and designated senior leader will supervise a proportionate investigation.
- Statements or accounts may be gathered from the students and staff involved and from witnesses where appropriate.
- Relevant digital evidence may be reviewed in accordance with school procedures and applicable privacy and safeguarding requirements.
- Parents/guardians will be informed as appropriate.
- The school will decide the required action, which may include educational, restorative, pastoral, disciplinary, or safeguarding responses.
- Serious incidents may be escalated to the Principal and, where required, relevant external or regulatory authorities.
- Students affected by digital harm will receive appropriate support and follow-up.
- Each incident will be reviewed after an agreed period, based on its nature and the needs of those involved.

Possible Strategies to Support Students

- Reassurance and immediate safeguarding support.
- Counselling or pastoral support.
- Digital citizenship education and targeted guidance.
- Support with privacy, account security, and reporting tools.
- Restorative approaches where appropriate and safe.
- Peer support or mentoring where suitable.
- A structured monitoring or reintegration plan where required.

Sanctions for Digital Misuse

The school's response will be proportionate to the nature and seriousness of the incident, the student's age and circumstances, previous incidents, safeguarding considerations, and applicable school procedures. Possible responses may include:

- Verbal reminder or warning.
- Parent/guardian communication.
- Written warning.
- Temporary restriction or loss of access to specified digital privileges or activities.
- Behaviour support plan or structured monitoring.
- Counselling, digital citizenship education, or restorative intervention.
- Suspension or other serious disciplinary action in accordance with school procedures.
- Permanent exclusion/termination of enrolment where warranted and in accordance with applicable requirements.
- Referral to relevant authorities where required.

Positive Strategies for Responsible Digital Behaviour

- Students will be helped to understand how their digital choices affect themselves and others.
- Students will be encouraged to take responsibility and identify safer, more respectful alternatives.
- Students may be given opportunities to demonstrate positive digital citizenship and contribute to awareness initiatives.

- Where appropriate, students may be supported to repair harm through a genuine apology or restorative process.
- Will arrange counselling or targeted support where required.

Staff Responsibilities

- Model safe, respectful, ethical, and purposeful digital behaviour.
- Teach and reinforce digital citizenship and responsible technology use.
- Protect confidential and sensitive information.
- Report safeguarding and digital concerns promptly.
- Use approved digital systems and follow school procedures for accounts, devices, data, and online learning.
- Verify AI-generated information before using it in professional contexts.
- Support students to use AI critically and responsibly rather than simply prohibiting technology without educational purpose.

Review and Monitoring

DPS RAK will monitor the effectiveness of this policy through digital incident records, safeguarding reviews, student and parent feedback, staff feedback, digital citizenship activities, technology audits, and relevant school improvement processes. Emerging risks and developments in digital technology and AI will be considered during policy review and staff/student awareness planning.

Whole-School Commitment

DPS RAK is committed to ensuring that technology remains a positive, safe, inclusive, and purposeful part of school life. We rely on trust, respect, responsible communication, critical thinking, digital literacy, and partnership between students, staff, parents, and the wider school community. Everyone shares responsibility for creating a safe digital environment in which technology enhances learning and wellbeing.

Key Expectations at a Glance

- Use technology safely, respectfully, responsibly, and for authorised purposes.
- Protect passwords, personal information, privacy, and others' digital identities.
- Do not bully, harass, threaten, impersonate, or deliberately harm others online.
- Do not access, create, or distribute inappropriate or harmful content.
- Respect copyright, intellectual property, and academic integrity.
- Report digital safeguarding concerns promptly to a trusted adult.
- Use AI transparently, critically, ethically, and only as permitted for the task.
- Never enter confidential or sensitive information into unauthorised AI tools.
- Remember that you remain responsible for work created or submitted with digital or AI assistance.
- Use technology to enhance learning, creativity, collaboration, wellbeing, and positive digital citizenship.

Policy Administration

Prepared & Reviewed by:	Senior Management Team	Last Review date:	March 2026
Next Review date:	March 2027	Authorized by	School Principal
Policy Title	Digital Usage Policy	No. of Pages:	7

