SALWAN MONTESSORI SCHOOL

Gurugram

School Technology, Digital Citizenship & AI-Use Policy

Effective: 1 April 2026

Next Review: March 2027

Public Version · For Parents, Students & Community

Approved by: School Principal & IT Head

Aligned with: DPDP Act 2023, NEP 2020, CBSE Guidelines, IT Act 2000

And UNESCO’s framework for use of AI by students and teachers.

Purpose & Scope

This policy governs the safe, responsible, and ethical use of all school-provided and personally owned technologies. It applies to students, parents/guardians, and staff using school networks, devices, learning platforms, or approved educational technologies- including Artificial Intelligence (AI) tools.

Our goal is to empower the school community to use technology safely, creatively, and thoughtfully, fostering digital literacy, academic integrity, and respect for others.

1. This Policy Covers

This policy covers:

- School computers, tablets, smart boards, and interactive panels
- Internet and Wi-Fi access on campus
- Learning Management Systems (LMS), ERP, and EdTech platforms
- AI-based learning tools approved by the school
- Personal devices (BYOD) connected to the school network

Responsibilities of Students

Students Must

- Use technology for school-approved educational purposes only, under teacher supervision.
- Keep login credentials private and never share passwords.
- Respect intellectual property, no plagiarism or uncredited AI-generated content.
- Handle devices with care and maintain good digital hygiene (log off, update software, report issues).
- Use respectful language in all online communication.

- Report any damage, security concerns, or suspicious activity immediately.
- Use Interactive Flat Panels (IFPs) only for collaborative study; keep them off without teacher permission or in the absence of teacher.
- Build a Positive Digital Footprint: Every post, comment, and search contributes to your permanent digital reputation. Aim to leave a trail of kindness and intellectual curiosity.

Students Must NOT

- Access or share offensive, inappropriate, or illegal content.
- Attempt to bypass firewalls, filters, or monitoring systems.
- Install unauthorized apps, games, or extensions.
- Use AI to cheat, plagiarize, or avoid genuine learning.
- Record, photograph, or share school content without permission.
- Engage in cyberbullying or disclose personal/private data online.

2. **Responsibilities of Parents & Guardians**

Parents are vital partners in promoting digital safety. You are expected to:

- Parents are expected to monitor and guide their child's use of technology and AI at home, ensuring age-appropriate engagement, parent-led use at the primary level, supervised exploration in middle school, and responsible, disclosure-based use in senior school.
- Encourage ethical digital citizenship and age-appropriate online behaviour.
- Report concerns related to online safety or misuse to the school promptly.
- Support your child's digital well-being at home with simple, consistent practices: limit recreational screen time to 1 hour per day for school-

going children; ensure AI tools (such as ChatGPT or Gemini) are used only for learning with parental awareness and not for completing assignments independently; prefer age-appropriate, school-recommended apps; keep devices in common areas during study hours; and have regular conversations about what your child is doing online.

- Use parental control features built into your child's device (Screen Time on iOS, Digital Wellbeing on Android) to set daily app limits, schedule device-free hours, and block inappropriate content. Consider enabling Focus/Zen Mode during study and sleep hours. For younger children, apps like Google Family Link or Microsoft Family Safety allow remote monitoring and approval of app downloads.
- Avoid early exposure to social media platforms-most require users to be at least 13 years old while others as 16 years. Parents ensure that they do not give consent for joining social media and other platforms before the prescribed age.
- Parental consent is required for use of school-approved ERP, LMS, and AI tools. Consent can be withdrawn anytime in writing.

3. Responsibilities of Teachers & Staff

- Model responsible technology use and always uphold academic integrity.
- Integrate digital tools and AI ethically to enhance and not replace critical thinking.
- Educate students about online safety, digital footprints, and data privacy.
- Supervise student digital activity during class and report misconduct.

- Protect student information in compliance with the Digital Personal Data Protection Act (2023) and relevant international standards.
- Guide students to engage with AI responsibly, following evidence-based best practices that improve learning outcomes.

4. Data Privacy & Protection

- The school collects only essential student data for educational purposes.
- Data is stored securely and not shared without consent.
- While the School implements appropriate technical and organisational measures to safeguard data, any unforeseen incident such as loss, unauthorised access, accidental disclosure, or cyber events (including ransomware or hacking attempts) will be addressed with due diligence and urgency. School will take immediate steps to contain and mitigate the impact of the incident. School will inform such cases to relevant authorities.
- Never share personal or sensitive information online such as Aadhaar numbers, home addresses, or private phone numbers, on any digital platform.
- Parents may request correction or deletion of data as permitted by law.Parents or students with privacy-related concerns may address them to the IT department of the school through the school's official communication channels.
- Use of Third-Party Platforms (EdTech/AI Tools):
    - The School may engage third-party educational technology platforms to support teaching and learning processes, with prior parental consent wherever required. In such cases, the School

undertakes reasonable due diligence, including privacy and security assessments, before onboarding any platform.

- All such service providers are required to process student personal data strictly for legitimate educational purposes, in accordance with applicable law and the school's instructions. They shall not use such data for profiling, targeted advertising, marketing, behavioural tracking, or any unrelated commercial purposes.
- The school ensures that appropriate contractual safeguards are in place with such vendors to maintain confidentiality, security, and compliance with the provisions of the Digital Personal Data Protection Act, 2023. For any unforeseen hacking/data leak at the end of third party vendor, school shall not be held responsible.

5. Responsible Use of Devices

School Devices

- Used only for academic purposes under supervision.
- System settings must not be modified by students.
- Any damage must be reported immediately; negligence may result in cost recovery.

Personal Devices (BYOD)

- Allowed only with prior written approval, for specific academic tasks.
- Must connect only to the secured school Wi-Fi network; updated antivirus required.
- The school is not liable for loss or damage of personal devices.

Mobile Phones & Wearables

⚠ Mobile phones and internet-enabled wearables (smartwatches, etc.) are NOT permitted during school hours unless explicitly authorized by the principal.

6. **Artificial Intelligence (AI) Use Guidelines**

- Always disclose when AI has been used in assignments or projects.
- Always verify the accuracy of AI outputs; AI can be wrong or biased.
- Use only school-approved AI platforms.
- Never upload personal data to any AI platform.
- Age-Differentiated Technology & AI Use: In line with CBSE and NEP 2020 guidance, technology and AI exposure is tailored to developmental stage:
  - Primary (Grades 1–5): Guided, teacher-led use only. No independent AI accounts or unsupervised digital activity.
  - Middle School (Grades 6–8): Supervised exploratory use of approved platforms, with teacher oversight and structured learning objectives.
  - Senior School (Grades 9–12): Responsible, disclosure-based use. Students are expected to cite AI tools used, exercise critical evaluation of AI outputs, and demonstrate original thinking.

7. **Algorithmic Fairness & Bias Awareness (AI Use)**

- The school recognizes that AI-generated outputs may contain bias, inaccuracies, or incomplete information. Students and staff are guided to critically evaluate such outputs.
- The school does not permit the use of AI tools for high-stakes decisions (such as grading, discipline, or student evaluation) without appropriate human oversight and professional judgement.

8. Academic Integrity

- Academic honesty is non-negotiable:
- Submitting copied or AI-generated work without citation is malpractice.
- Plagiarism and digital misconduct will result in disciplinary review.
- Students may be asked to demonstrate understanding through viva voice or supervised re-assessment.

⚠ AI-detector results alone will not be used as disciplinary evidence- contextual review will always apply.

9. Internet Safety & Digital Well-Being

- Avoid responding to unsolicited messages or clicking on suspicious links.
- Report cyberbullying, fake accounts, or harmful content immediately to a teacher or ICT Coordinator.
- Students should maintain a healthy balance between screen time and offline activities, while developing awareness of risks such as online addiction, doom scrolling, and over-dependence on AI. Students and parents are encouraged to approach the school counsellor or class teacher proactively if they observe signs of digital distress or compulsive technology use.
- Change passwords frequently of your mail and other accounts and do not keep an easy to guess platform. It must be a combination of uppercase letters, lowercase letters, numbers, and special symbols.

10. Social Media Conduct

- Do not post school-related content, images, or videos without explicit permission.
- Refrain from misusing the school's name, logo, or identity on personal social media accounts.
- Always represent yourself and the school respectfully online.
- Student images and names are published on official school social media only with annual written parental consent.

11. Monitoring & Enforcement

- All school networks and devices are monitored for cybersecurity and policy compliance. The school may restrict access to platforms that pose safety or privacy risks.

  Violations may lead to:

  - Counseling or warnings
  - Suspension of technology access
  - Device confiscation
  - Financial restitution for damages
  - Disciplinary or legal action for serious breaches
  - School will not provide Letter of Recommendation for placement or any other purpose to student defaulters of this policy.

12. IT Support & Helpdesk

For any technology-related concern-including device issues, access problems, suspected misuse, or online safety incidents, students and parents may contact the school's IT Helpdesk directly. Issues are acknowledged within one working day and resolved within three working days, with escalation to the IT Head or Principal for serious matters.

IT Helpdesk Email: itdept@salwangurgaon.com

13. Parent Consent for Digital Platforms & AI Tools (Parents provide it via form on ERP)

Parents/guardians must provide consent for use of school-approved ERP, LMS, and AI tools. By consenting, the parent acknowledges that:

- The school collects only essential student data for educational purposes.
- No sensitive personal data is shared with external parties without explicit consent.
- AI use will occur under teacher supervision and full transparency.
- Consent can be withdrawn at any time in writing to the school office.
- Consent forms are collected digitally through the School ERP/Almanac/ Forms available at the beginning of each academic session.

14. Student Digital Citizenship Pledge (Class Teacher obtain signed copy of the pledge from the students)

I promise to:

- Use technology responsibly- for learning, not distraction.
- Be honest and give credit where it is due.
- Protect my passwords and personal information.
- Be respectful and kind in all online interactions.
- Avoid cyberbullying and refrain from sharing inappropriate content.
- Treat all devices with care and report problems promptly.
- Use AI thoughtfully, as a thinking partner, not a shortcut.

I acknowledge that I have understood the School Policy. I am taking this pledge with due understanding, and any violation of this pledge may result in disciplinary action, suspension of technology access, and/or loss of opportunities and privileges at school, as deemed appropriate by the school authorities.

Student Name: _____

Class & Section: _____

Signature: _____

Date: _____

Parent/Guardian Signature: _____

Date: _____

15. Review, Governance & Alignment

This policy aligns with best practices from established educational technology and data protection frameworks.

It will be reviewed annually to remain current with the latest Digital Personal Data Protection Act and evolving AI-in-education research.

Approved by: School Principal and IT head

Effective Date: [1st April 2026]