



ICT & Digital Safety Policy

SCHOOL POLICY · DRAFT FOR REVIEW · JULY 2026

JYOTI MODEL SR. SECONDARY SCHOOL, Adarsh Nagar, Delhi

Affiliated to CBSE — School Code: 1309228

Guided by our motto: "Work is Worship"

1. Preamble

At JYOTI MODEL SR. SECONDARY SCHOOL, we recognise that technology is an indispensable tool for learning, creativity, communication and innovation in the 21st century. Our ICT and Digital Safety Policy provides a comprehensive framework for the responsible, ethical and safe use of technology by all members of the school community — students, teachers, staff and, where applicable, parents and visitors.

This policy is guided by the principles of:

- **Safety:** Protecting students from harm in digital environments
- **Responsibility:** Encouraging ethical, lawful and considerate use of technology
- **Empowerment:** Equipping students with the digital skills they need to thrive
- **Partnership:** Working with parents to extend digital safety practices beyond the school gates

This policy applies to all devices and networks owned or managed by the school, as well as personal devices used on school premises or for school-related activities. It applies during school hours, at school events and on school-organised trips.

2. The School's ICT Infrastructure

JYOTI MODEL SR. SECONDARY SCHOOL maintains a modern ICT infrastructure designed to support teaching, learning and administration:

- **Computer Laboratory:** A fully equipped lab with networked computers loaded with curriculum-relevant software, internet access and printing facilities. The lab is used for dedicated ICT classes, research projects and cross-curricular digital activities under the supervision of a qualified computer instructor
- **Smart Classrooms:** Select classrooms are equipped with interactive smart boards or projection systems connected to the school network, enabling teachers to integrate multimedia content, simulations, virtual labs and digital assessments into daily lessons

- **School Network:** A secure, filtered Wi-Fi network covers administrative areas and designated learning spaces. Internet access is governed by a firewall and content filtering system that blocks inappropriate, harmful or distracting websites and content categories
 - **Administrative Systems:** Student records, attendance, examination data and fee records are maintained on secure, password-protected digital platforms accessible only to authorised staff members
 - **School Website & Social Media:** The school maintains an official website (www.jyotimodelschool.com) and official social media accounts as platforms for information, celebration and community engagement. All content published on these platforms is reviewed and approved by the school leadership
-

3. Computer Laboratory Rules

The computer laboratory is a shared learning space. All users must adhere to the following rules:

Access and Supervision

- The computer lab is accessible to students only during scheduled class periods under the direct supervision of the computer instructor or a designated teacher
- Unscheduled use of the lab requires prior permission from the computer instructor or Principal
- During practical examinations, CBSE-prescribed protocols are strictly followed

Acceptable Use

- Students may only access websites, applications and software prescribed or approved for educational purposes
- Logging in with another student's credentials is strictly prohibited
- Each student must log out of their session at the end of the period
- Printing is permitted only with teacher authorisation and for academic purposes
- Students must save their work to designated network folders or school-provided cloud storage — saving to the local hard drive is discouraged

Prohibited Activities

The following activities are strictly prohibited in the computer laboratory and on any school-managed device:

- Downloading, installing or running any unauthorised software, games, executables or browser extensions
- Accessing, viewing or distributing content that is pornographic, violent, hateful, discriminatory or otherwise inappropriate

- Attempting to bypass, disable or circumvent the school's content filtering system, firewall or security protocols
- Unauthorised attempts to access another user's files, accounts or data
- Damaging, tampering with or misusing hardware, peripherals, cables or network equipment
- Eating, drinking or bringing food items into the computer laboratory
- Using the lab for commercial purposes, gambling or any illegal activity

Care of Equipment

Students are expected to treat all ICT equipment with care. Any damage — accidental or otherwise — must be reported immediately to the lab instructor. Students found to have deliberately damaged equipment may be required to bear the cost of repair or replacement and may face disciplinary action.

4. Internet Safety Guidelines

The school employs multiple layers of protection to ensure a safe online environment:

Technical Safeguards

- A firewall with regularly updated content filtering blocks websites in categories including adult content, violence, hate speech, gambling, social networking (during class hours), file-sharing and known malware hosts
- All internet activity on the school network is logged. Logs are retained for a minimum of 90 days and reviewed periodically by the ICT Coordinator. Logs may be examined as part of any investigation into policy breaches
- Anti-virus and anti-malware software is installed on all school computers and updated regularly

Student Responsibilities

Every student is expected to follow these internet safety rules:

- Do not share personal information online — this includes full name, home address, phone number, date of birth, passwords, bank details or family information
- Do not share photographs or videos of yourself or other students without explicit teacher permission
- Do not arrange to meet anyone you have met online without parental knowledge and supervision
- If you encounter something online that makes you feel uncomfortable, scared or confused — close the screen and inform your teacher or the lab instructor immediately
- Never respond to abusive, threatening or inappropriate messages. Save the message and report it to a trusted adult

- Be mindful of your digital footprint — everything you post, share or comment online leaves a trace

Staff Responsibilities

Teachers and staff members are expected to:

- Model responsible digital behaviour at all times
 - Supervise students adequately during any online activity
 - Report any concerns about student online safety to the ICT Coordinator or Principal
 - Ensure that any digital content used in teaching is age-appropriate and curriculum-relevant
 - Use school-provided communication channels for all official correspondence with students and parents
-

5. Digital Citizenship Curriculum

Digital citizenship is integrated into our curriculum from the primary years through senior secondary. By the time a student graduates from JYOTI MODEL SR. SECONDARY SCHOOL, they will have been taught:

Primary Classes (I–V)

- What personal information is and why it should be kept private
- How to be kind and respectful when communicating online
- Recognising that not everything on the internet is true
- What to do if something online makes them feel uncomfortable
- The importance of balance between screen time and other activities

Middle School (VI–VIII)

- Responsible social media use and managing online privacy settings
- Identifying misinformation, fake news and clickbait
- Understanding and respecting copyright, fair use and Creative Commons
- Cyberbullying: recognising it, responding to it and reporting it
- Digital footprint: understanding that online actions have lasting consequences
- Online grooming awareness: recognising manipulative behaviour from strangers

Secondary & Senior Secondary (IX–XII)

- Advanced privacy and security practices (password hygiene, two-factor authentication, recognising phishing)
- Ethical dimensions of technology: plagiarism, intellectual property, AI ethics
- Impact of social media on mental health and body image

- Digital activism, civic engagement and responsible online discourse
 - Career and academic use of digital tools (LinkedIn, academic databases, portfolios)
 - Understanding Indian IT laws and cybercrime legislation
-

6. Mobile Phone and Personal Device Policy

For Students

- Students are not permitted to use mobile phones, smartwatches with communication capabilities, or any personal electronic device during school hours
- If a student needs to carry a mobile phone for safety reasons (e.g., travelling long distances), the phone must be switched off and deposited with the class teacher at the start of the school day. It will be returned at the time of dispersal
- Any student found using a mobile phone during school hours without prior authorisation will have the device confiscated. The device will be returned only to a parent or guardian
- Repeated violations may result in disciplinary action, including a letter of concern placed in the student's file
- The school is not responsible for the loss or damage of any personal device brought to school

For Teachers and Staff

- Teachers and staff may use personal mobile phones during break times and for school-related communication
- Personal phone use during teaching hours is discouraged. Teachers are expected to keep phones on silent and attend to urgent calls only during non-instructional time
- Staff members must not use personal phones to photograph or record students except for authorised school activities with prior permission from the Principal

For Parents and Visitors

- Parents and visitors are requested to keep mobile phones on silent mode while on school premises
 - Photography or videography of students by visitors is not permitted without explicit prior authorisation from the school office
 - Parents may contact their child during school hours only through the school office, which will relay messages as needed
-

7. Data Protection and Privacy

The school takes the privacy and security of student and staff data seriously:

Student Records

- Student personal data (admission forms, academic records, medical information, attendance, contact details) is stored in secure, password-protected digital systems with role-based access control
- Only staff members with a legitimate educational or administrative need may access student records
- Student data is never shared with third parties for commercial or marketing purposes
- Academic records are retained as per CBSE guidelines and destroyed securely when no longer required

Photographs and Student Work

- The school may take photographs and videos of students engaged in school activities for use in the school website, social media, newsletters, brochures and other official publications
- Written consent is obtained from parents at the time of admission for the use of student images and work in school publications
- Parents may withdraw consent at any time by notifying the school office in writing
- Student work (artwork, projects, writing) may be displayed within the school or on the school website with the student's name, unless parents request otherwise

Digital Communication

- Official school communication with parents is conducted through the school diary, official school email, school website and authorised parent communication apps
- Teachers and staff must not share student photographs, results or personal information on their personal social media accounts
- Group communication apps used for parent-teacher communication must be set up and monitored by the school administration

8. Social Media Guidelines

School Social Media Accounts

The school maintains official social media accounts on platforms including Instagram (@jmsss_official), YouTube and Facebook. These accounts are managed by designated staff members and used to:

- Celebrate student achievements and school events
- Share important announcements and circulars
- Highlight the school's academic, co-curricular and community activities
- Build a positive online presence for the school community

Prohibited Online Conduct by Students

Students must not:

- Create fake accounts impersonating the school, its staff or other students
- Post content that defames, harasses or threatens the school, its staff or students
- Share school-related confidential information (results, disciplinary matters, internal communications) on public platforms
- Engage in online arguments or conflicts involving the school's name

Where online misconduct by a student comes to the school's attention — even if it occurs outside school hours or on personal devices — the school reserves the right to investigate and take appropriate action, recognising that online behaviour can significantly affect the school environment.

9. Policy Breaches and Consequences

Any breach of this ICT & Digital Safety Policy is treated seriously. Consequences are applied on a case-by-case basis, taking into account:

- The nature, severity and frequency of the breach
- The student's age, understanding and previous disciplinary record
- Whether the breach caused harm to another person or to school property
- Whether the breach involved illegal activity

Range of Consequences

Depending on the above factors, consequences may include:

- A verbal warning and educational conversation about responsible technology use
- Temporary or permanent loss of computer lab or internet access privileges
- A written letter to parents informing them of the breach
- Confiscation of personal devices (returned to parents only)
- Detention, community service within the school or other restorative measures
- Suspension from specific activities or technology-related programmes
- In cases involving illegal activity (hacking, cyberbullying, access to illegal content): suspension, expulsion and/or referral to law enforcement

Procedure

1. Any staff member who becomes aware of a breach reports it to the ICT Coordinator and class teacher
2. The ICT Coordinator investigates and documents findings
3. The class teacher and/or Principal decides on appropriate consequences in consultation with the ICT Coordinator

4. Parents are informed of the breach and consequences applied
 5. A follow-up conversation is held with the student to reinforce learning and prevent recurrence
-

10. Roles and Responsibilities

The School Leadership (Principal / Chairperson) is responsible for:

- Approving this policy and ensuring its implementation
- Allocating resources for ICT infrastructure, maintenance and training
- Ensuring that the policy is reviewed annually

The ICT Coordinator is responsible for:

- Maintaining the school's ICT infrastructure, network security and content filtering systems
- Supporting teachers and students in the effective use of technology
- Investigating and documenting policy breaches
- Recommending improvements to the policy based on emerging technologies and threats

Teachers and Staff are responsible for:

- Supervising students during technology use
- Integrating digital citizenship into their teaching
- Modelling responsible technology use
- Reporting any concerns or breaches promptly

Students are responsible for:

- Following this policy at all times when using school technology
- Reporting any safety concerns or policy breaches they witness to a trusted adult
- Using technology as a tool for learning, creativity and positive contribution

Parents are responsible for:

- Reading and discussing this policy with their children
 - Supporting the school in reinforcing responsible technology use at home
 - Reporting any technology-related concerns involving their child to the school
-

11. Policy Review

This policy is reviewed annually by the school leadership team in consultation with the ICT Coordinator, teachers and, where appropriate, students and parents. It is updated to reflect:

- Changes in technology and digital platforms used by students
- Emerging online safety threats

- Changes in CBSE or government guidelines and legal requirements
- Feedback from staff, students and parents

The review date and version number are recorded below:

Version	Date	Summary of Changes	Reviewed By
1.0	July 2026	Initial policy	School Leadership

12. Related Documents

This policy should be read in conjunction with:

- Anti-Bullying Policy (includes cyberbullying provisions)
- Safety & Security Policy
- Student Code of Conduct
- Acceptable Use Agreement (signed by students and parents at admission)
- CBSE guidelines on ICT in schools

For questions or concerns regarding this policy, please contact the school office at info@jyotimodelschool.com or call 011-2768 2469.