



**D.A.V. Public School, Vasant Kunj, New Delhi**



# Cyber Policy

## VISION

"At DAV Public School Vasant Kunj, we believe that cyber safety is a shared responsibility. By fostering a culture of respect, responsibility, and vigilance online, we empower our students and teachers to navigate the digital world safely and ethically."

## OBJECTIVE

The objective of DAV Public School Vasant Kunj's Cyber Policy is to create a secure, respectful, and responsible digital environment that maximizes the educational benefits of technology while minimizing and managing its risks. This policy aims to educate and guide students and staff on safe internet practices, protect personal information, and ensure a positive online experience, thereby supporting student learning outcomes and the effective operation of the school.

## NEED OF A CYBER POLICY

To safeguard information and IT infrastructure in cyberspace, develop robust capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents. Achieve this through a strategic combination of institutional structures, skilled personnel, efficient processes, technology and strong cooperation.



**D.A.V. Public School, Vasant Kunj, New Delhi**



### **GUIDELINES FOR STUDENTS**

1. **Protect Personal Information:** Do not share personal details such as your passwords, photograph, address, phone number, or any other personal information online without teacher or parental permission.
2. **Use Strong Passwords:** Create strong passwords that are difficult to guess. In combination with Special characters & minimum 1 capital letters with numbers to make the password strong. Keep them confidential.
3. **Do not bring equipment such as iPad, iPod, PSP, mobile phones etc. to the school without approval from the school administration. Any such equipment found without prior approval will be confiscated and kept with the school authorities.**
4. **Respect Online Etiquette:** Always be respectful and courteous when communicating online. Avoid any form of bullying, harassment, or inappropriate behavior.
5. **Report Suspicious Activity:** Inform a teacher or school administrator immediately if you encounter anything online that makes you uncomfortable or seems suspicious.
6. **Be Aware of Digital Footprint:** Remember that everything you post online can be traced back to you and can affect your future. Think before you post.

## **What happens if a student breaches DAV Public School's Cyber Policy?**

1. Investigation: Any suspected breach of the CyberSafety Policy will be promptly investigated by school authorities.
2. Notification: Parents or guardians will be notified of the breach and the details of the incident.
3. Consequences: Consequences for breaching the policy may include, but are not limited to:
  - Verbal or written warning
  - Temporary or permanent suspension of internet privileges
  - Detention or other disciplinary actions
  - In severe cases, suspension or expulsion from school
4. If you behave online in a manner that threatens the well-being of another child, student, parent or member of the school community, even if this occurs off-site and or out of school hours, the Principal/Supervisory Head has the authority to take appropriate action.
5. When it is suspected that a personal electronic device such as a mobile phone is used to capture images of a crime (such as an assault), or contains any other evidence of a crime, the device will be confiscated and handed to the police.
6. If the Principal suspects an electronic crime has been committed, this will be reported to the Police Department. Where there is a further reasonable suspicion that evidence of a crime, such as an assault, is contained on a mobile phone or other electronic device such as a notebook computer etc., the device will be confiscated and handed to the investigating police officer. The Police will determine any further action.
7. These actions may be taken even if the alleged incident occurs off-site and/or out of school hours.

8. **Education and Remediation:** The student may be required to attend a cyber safety education session to understand the risks and responsibilities associated with internet use.
9. **Support:** Counseling and support services will be available to help students understand the implications of their actions and to promote better online behavior in the future.
10. **If the breach caused damage or harm,** the student may be required to make restitution or make actions to rectify the situation.

## **GUIDELINES FOR TEACHERS**

1. **Supervise Internet Use:** Actively monitor students' use of the internet during school hours to ensure they are following the CyberSafety Policy.
2. **Educate Students:** Teach students about the importance of internet safety, digital citizenship, and the potential risks of online activities.
3. **Enforce Rules Consistently:** Apply the CyberSafety Policy consistently and fairly to all students.
4. **Provide Safe Resources:** Recommend and use age-appropriate and safe online resources for educational purposes.
5. **Be a Role Model:** Demonstrate positive online behavior and lead by example.

## **GUIDELINES FOR PARENTS**

1. Place the computer in an open area in your home - not in your children's bedroom.
2. Set clear expectations for your children, based on age and maturity.
3. Install parental control (content filtering) software.
4. Learn Internet basics, be approachable and lead by example.

## **TIPS FOR PARENTS TO AVOID AND IDENTIFY CYBER BULLYING**

1. Discuss any changes in mood or behavior with them. If you are concerned, help your child to stay connected to friends and family members they trust.
2. Talk to your child about Cyberbullying before it happens.
3. Be aware of what your child is doing online and explore it with them.
4. Keep the lines of communication open so your child will be comfortable talking about if something is worrying them. Help your child to develop the skills they

need to interact safely and respectfully online. Guide their online activities and help them learn to communicate appropriately with friends and family.

5. Help your child to block anyone who sends offensive content. Most social networking services allow users to block and report someone who is behaving badly.

*"Cyberbullying won't cease if ignored – support your child by listening to them and helping them take control of the situation."*

### **Guidelines to Use Internet Safely in School Premises**

1. Access Approved Websites Only: Only visit websites that have been approved by teachers or the school administration for educational purposes.
2. Avoid Unsupervised Browsing: Do not browse the internet without the supervision of a teacher or a responsible adult.
3. Do Not Download Unauthorized Software: Refrain from downloading or installing software, apps, or any digital content without permission.
4. Use School Devices Responsibly: Handle school-provided devices with care and use them solely for educational purposes.
5. Log Out After Use: Ensure you log out from any accounts and close all applications properly after using school computers.

By adhering to these guidelines, we aim to create a safe and supportive online environment for all members of the DAV Public School Vasant Kunj community.