



DELHI PRIVATE SCHOOL, AJMAN

PB No: 21900, Al Tallah 2, Ajman, U.A.E, Phone: 06-747 1111,
Email: info@dpsajman.com, website: www.dpsajman.com

Online Safety Policy

1. Introduction

The Online Safety Policy of Delhi Private School Ajman ensures that all students, staffs, parents and other stakeholders of the school are able to use the internet and related communication technologies appropriately and safely. This policy is linked with all other relevant policies meant for cyber security i.e. Acceptable Use Policy, Filtering Policy, Anti-Cyber Bullying Policy, Child Protection Policy, Health and Safety Policy, Password Security Policy and Behavior Management Policy.

The OSP aims to facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase accomplishment, keep students and stakeholders safe and prepare students for the dangers and opportunities of today's and tomorrow's digital world, to survive and succeed online. This policy also aims to help all the stakeholders of the school to understand their roles and responsibilities to be a digital citizen.

2. Scope of the Policy

The Online Safety Policy applies to all the stakeholders of Delhi Private School Ajman (including students, parents, staffs, and visitors) who have access to the school network, digital technology, whether directly or remotely, and at any time.

The school will deal with concerns regarding online safety of students/staff in and out of the school as mentioned within this policy and associated policies and will, where known, inform parents and in critical cases, inform external agencies, regarding the inappropriate online safety behavior that take place in or that is associated with DPS Ajman.

3. Policy Statements

3.1. Education – Students

Online Safety of students is an essential part of the school's online safety strategies that focuses on educating students to take a responsible approach. DPSA helps the students to recognize and avoid online safety risks and build their resilience.

At DPSA, we make sure that online safety is a focus in the curriculum and that all staff members are reinforcing online safety messages across the curriculum, especially in ICT curriculum. The online safety curriculum is designed in a way that it provides progression, with opportunities for creative activities in the following ways:

- 3.1.1 Key online safety messages will be reinforced as part of the assemblies.
- 3.1.2 Students will be taught in lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- 3.1.3 Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet as mentioned in the Acceptable Use Policy for Students (ANNEXURE 1,2 & 3 Points 1.4, 2.4 & 3.4, respectively) of the school.
- 3.1.4 Students will be supported in building resilience by providing a safe environment for debating on issues and helping them to understand how they can influence and participate in decision-making and updating the policies of the school.
- 3.1.5 Students will be helped to understand the need for the Acceptable Use Policy for Students and encouraged to adopt safe and responsible use both within and outside school.
- 3.1.6 Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- 3.1.7 In lessons where internet is used, students will be guided to sites which are as suitable for their use and that processes are in place for taking action with any unsuitable material that is found in internet searches. (Acceptable Use Policy for Staff – ANNEXURE 5 – Point 5.13)
- 3.1.8 Where students are allowed to freely search the internet, staff members will be vigilant in monitoring the content of the websites the students visit.

- 3.1.9 It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would result in internet searches being blocked. In such a situation, staff can request that the IT in-charge to temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, stating the need for the access. (Acceptable Use Policy for Staff – ANNEXURE 5 – Point 5.14)
- 3.1.10 BYOD will be implemented with effect from May 2022, phase wise to ensure the best and safe use of educational technology.

3.2. Education – Parents

Many parents may only have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviors. Parents may underestimate how often their children stumble across potentially harmful and inappropriate material on the internet and may not be sure how to respond when they come across such concerns.

The school will provide information and awareness to parents through:

- Awareness sessions by the Online Safety Leader
- Emails, newsletters, web site, Learning Platform

3.3. Education & Training – Staff

It is mandatory for all staff to undergo online safety training provided by the school and understand their responsibilities, as outlined in this policy.

- 3.3.1 A formal online safety training will be made available to staff. This will be regularly updated and reinforced.
- 3.3.2 All new staff will receive online safety training as part of their induction program, ensuring that they fully understand and sign the schools' Online Safety Policy and Acceptable Use Policy.
- 3.3.3 The Online Safety Leader will receive regular updates through attendance at external training events.

- 3.3.4 Staff will be given the opportunity to discuss the Online Safety Policy and its updates.
- 3.3.5 The Online Safety Leader will provide advice/guidance/training to staff members as required.
- 3.3.6 Teachers undergo regular training from CBSE and HRDC sessions from DPS Society.
- 3.3.7 All teachers will acquire certificates from Khalifa Empowerment Program – Aqdar.
- 3.3.8 Regular sessions on Digital Citizenship and Online Safety will be organized for students, staff and parents in coordination with Ajman Police.

4. Roles and Responsibilities

The following are the roles and responsibilities of students/ staff members/ parents and all other stakeholders of the school regarding online safety:

4.1. Principal and Senior Leaders:

- 4.1.1 The Principal will ensure the online safety of members of the school community, through Online Safety Group and the Online Safety Leader.
- 4.1.2 In the event of a serious online safety allegation being made against a member of staff, the concern will be escalated to the Principal.
- 4.1.3 The Principal will ensure through OSG that there is a system in place to allow for monitoring and support of those in school (teachers/e-COPS) who carry out the internal online safety monitoring role.
- 4.1.4 SLT members will ensure the regular training of staff in coordination with the ICT teachers
- 4.1.5 SLT members will ensure that the action point discussed in the OSG meetings are carried out promptly.

4.2. Online Safety Leader:

The Online Safety Leader has a daily responsibility for the online safety of all the stakeholders of the school. The OSL will:

- 4.2.1 take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school's online safety policies / documents.
- 4.2.2 keep up-to-date with new developments in the area of online safety and child protection.

- 4.2.3 take action on the online safety concerns as mentioned in the Student Behaviour Management Bylaws given by the Ministry of Education.
- 4.2.4 ensure that all discussions in the Online Safety Group meeting ends with a decision, action or definite outcome.
- 4.2.5 investigate the online safety concern thoroughly and take action accordingly.
- 4.2.6 ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- 4.2.7 focus on child protection and awareness among the students.
- 4.2.8 provide training and guidance for all the stakeholders of the school.
- 4.2.9 monitor the safe use of data across the school.
- 4.2.10 liaise with the Local Authority / relevant body in case of sensitive concerns related to online safety.
- 4.2.11 conduct regular meeting with the e-COPS and empower the e-COPS to induct the new students.
- 4.2.12 liaise with the school technical staff.
- 4.2.13 receive reports of online safety incidents and creates a log of incidents to inform future online safety developments.

4.3. In-charge of IT department:

The In-charge of IT department will be a part of Online Safety Group and is responsible for ensuring:

- 4.3.1 that the school's technical infrastructure is secure as possible and is not open to misuse or malicious attack.
- 4.3.2 that users may only access the networks and devices through a properly enforced Password Security Policy.
- 4.3.3 the filtering of websites is applied and updated on a regular basis.
- 4.3.4 that they keep up to date with online safety technical information provided by the MOE or other government agencies.

4.3.5 that the use of the network/internet/learning platform/remote access/email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Leader for investigation.

4.4. Teaching and Support Staff

Are responsible for ensuring that:

4.4.1 they have an up-to-date awareness of online safety measures and of the current school Online Safety Policy and practices.

4.4.2 they have read, understood and signed the Acceptable Use Policy, Health and Safety Policy, and Password Security Policy.

4.4.3 they report any suspected misuse or problem through the Pastoral Referral Form to the OSL for investigation and to take appropriate action.

4.4.4 all digital communications with students' parents should be on a professional level.

4.4.5 online safety issues are embedded in the curriculum and other activities.

4.4.6 students understand and follow the Online Safety Policy and other policies related to online safety.

4.4.7 students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

4.4.8 they monitor the use of digital technologies, mobile devices, cameras etc. in remote learning lessons and other school activities (where allowed) and implement current policies with regard to these devices.

4.4.9 in lessons where the internet is used, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

4.5. Students:

4.5.1 Are responsible to ensure that the school digital technology systems are used in accordance with the Acceptable Use Policy.

4.5.2 They have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- 4.5.3 They need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- 4.5.4 They report any online safety issues in the Incident Report Format for Students which is uploaded in their google classroom.
- 4.5.5 Students need to follow the reporting procedure as per the Reporting Posters (**ANNEXURE II,III & IV**) posted in each classroom.
- 4.5.6 They will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on taking / using images and on cyber-bullying.
- 4.5.7 Two students from the Cyber Club will be a part of the Online Safety Group
- 4.5.8 They should understand the importance of adopting good online safety practice when using digital technologies in and out of school and realize that the school's Online Safety Policy covers their actions out of school as well.

4.6. e-COPS

e-COPS are the facilitators of online safety who being the part of the school student community can better understand and help the other members of the online safety group in ensuring that the policies are followed.

Their roles include:

- 4.6.1. Ensuring that the students obey the guidelines provided by the school for online safety.
- 4.6.2. Monitoring the use of various digital technologies, mobile devices, apps, soft wares and portals students use for learning.
- 4.6.3. Two students from the e-COPS will be a part of the Online Safety Group
- 4.6.4. Bridging the gap (if needed) between the students and other members of online safety group.
- 4.6.5. Induct the new students on the AUP and other relevant policies and also inform the new students about the reporting procedures.
- 4.6.6. Reporting any incident that is against the policies to the Online Safety Leader and reporting any concerns that their classmates raise.
- 4.6.7. Communicating the problems faced by the students related to online learning.

4.6.8. Meeting and discussing various challenges faced as e-Cops with other e-Cops.

4.7. Parents:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Two members of the Parent Council will be a part of the Online Safety Group and they will also take sessions for the students on safety concerns and will be representing the school Online Safety Group at the Parent Council, if needed, to explain the plans set by the OSG for the session. The school will take every opportunity to sensitize parents to understand these issues through emails, newsletters, website / Learning Platform and information about national / local online safety programs. Parents will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events. Parents are suggested to continuously monitor their children's personal devices and their behavior to find out if they have been facing any concern like bullying and also to understand their online behavior. Parents are expected to report any online safety issues to the class teacher.

5. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, the school considers the following as good practice:

- 5.1. The official school communication with the students, staff, parents and other stakeholders will be through Microsoft 365 from May 2022.
- 5.2. The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- 5.3. Students' email ID's will be restricted to be used only within the organization. Students will neither be able to send mails nor they will be able to receive mails from outside the organization.
- 5.4. Users must immediately report, to the Online Safety Leader – in accordance with the Online Safety Policy.

- 5.5. Any digital communication between staff and students / pupils or parents / carers (email, social media, chat, blogs, etc.) must be professional in tone and content.
- 5.6. Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- 5.7. Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

6. Social Media

School has a responsibility provide a safe learning environment for pupils and staff. Staff members or students who harass, cyberbully, discriminate on the grounds of race or disability or who defame a third party will be liable to action as per the UAE laws.

- 6.1. The school does not support the use of social media accounts and staff should not use social media on school devices and are encouraged not to use social media on their own devices during school hours.
- 6.2. The school pro-actively monitors the internet for public postings about the school and responds to social media comments made by others according to a defined policy or process.
- 6.3. The school's use of social media for professional purposes will be checked regularly by the In-charge of IT department.
- 6.4. Responding to incidents of misuse by reporting immediately to the Online Safety Leader

7. IT Infrastructure

IT Infrastructure is becoming more relevant to support teaching, learning, assessment and administration in schools and DPS Ajman will be responsible for ensuring that the school IT infrastructure / network is as safe and secure as possible. With operation spread across school campuses, simplified, centralized management of the entire network. It also facilitates automation of previously manual processes, which leads to smooth running of our network. This also simplifies operations and reduces costs and risks.

While ensuring great student experiences and supporting student success is a primary focus, ensuring best IT experiences is important too, especially in today's campus where device proliferation and security concerns require detailed visibility and management of the network.

7.1. Structured Cabling

Foundation to any high-performance networks is the structured cabling to support the networks bandwidth, capacity, and power requirements. DPS Ajman installed CommScope Cat 6A copper cabling and Corning fiber cabling ensures the access layer foundation is ready and able with up to 10G speeds and support for High Power PoE. Corning's fiber solution provides the scalable bandwidth school's network backbone and for high performance applications like VR and Wi-Fi 6 Aps.

7.2. Wired and Wireless Network

DPS Ajman modernizes network infrastructure at its UAE schools to facilitate a fully integrated digital learning environment that elevates teaching and learning experiences of staff and students. Wireless network enables students and teachers to securely access Microsoft Office 365, Teams and other popular teaching, learning and collaboration applications without experiencing delay's, jitter, or dropped connections.

7.3. Foundation

DPS Ajman implemented an Aruba network architecture, enabling a state-of-the-art IT environment comprising infrastructure from CommScope Cat6A and Corning OM3 Fiber Cables. Aruba's diverse range of enhanced Network Access Control (NAC) solutions and security orchestration with ClearPass, as well as its High-Density Wi-Fi 6 access points and switches unified in a coherent design.

Implementing Aruba's wired and wireless networking solutions enabled the DPS Ajman to achieve 100% coverage across each of its school campuses without any blind spots, with 1000's of Wireless Access Points. This performance and reliability are pivotal for smooth operations as on average, over 15,000 devices connect to the network from across Group's five campuses.

7.4. BYOD

In a highly connected world, the diversity of digital devices and their personalized nature means that the DPS Ajman Group's staff and students would prefer to use their own devices for learning. All our campuses now support BYOD and implemented Zero trust architecture. Network Access Control has been key to supporting BYOD for staff and students in a truly secure manner.

7.5. Digitization Platform

The new network infrastructure forms the backbone of the schools' ongoing digitization program, supporting a wide range of devices including desktops, laptops, projectors, interactive display panels, iPads, CCTV systems, signage TV's, attendance, and access control systems.

7.6. MicroSoft 365 Education

Microsoft 365 Education empowers our teachers, students, and staff to unlock creativity, promote teamwork, and provide a simple and safe experience in a single, solution built specifically for education.

DPS Ajman invested in Microsoft 365 solution for all teachers, staff and students to improve the overall educational experience across the board in many ways as mentioned below:

- Promote teamwork and collaboration
 - It provides our staff a single hub for online connection and collaboration.
 - It meets the needs of individual students with a universal toolkit to share and communicate in and out of the classroom
- Unlock student creativity
 - Support creativity, collaboration, and problem solving with immersive and engaging apps to help students of all abilities become more independent with intelligent learning tools.

- Ensure safety and security
 - Microsoft 365 helps to manage users, data, and devices with a single dashboard.
 - It also helps to protect identity, apps, data, and devices with intelligent security enhanced by machine learning.

7.7. Technical Security

The school will be ensuring the safety and security of the school infrastructure / network and that policies and procedures within this policy are implemented. The staff members responsible for the security and safety of the students/ staff will also receive professional guidance and training, keeping in mind the following:

- 7.7.1 The technical requirements of the school will be met by the IT in-charge.
- 7.7.2 School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- 7.7.3 There will be regular reviews of the safety and security of school technical systems.
- 7.7.4 Wireless systems and cabling must be securely located and physical access restricted.
- 7.7.5 Appropriate security measures are in place to protect the firewalls, switches, routers, wireless systems, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- 7.7.6 Responsibilities for the management of technical security are clearly assigned to IT in-charge.
- 7.7.7 All users will have clearly defined access rights to school technical systems.

7.8. Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email(as mentioned in the Password Security Policy).

- 7.8.1 All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT in-charge and will be reviewed, at least annually, by the Online Safety Group.

- 7.8.2 All school networks and systems will be protected by secure passwords that are regularly changed
- 7.8.3 All users will have responsibility for the security of their username and password and they must not allow other users to access the systems using their log in details users must immediately report any suspicion or evidence that there has been a breach of security
- 7.8.4 Every user will have their own credentials to log in to their VLE, email and network.
- 7.8.5 Users are encouraged to change their passwords at regular intervals.
- 7.8.6 Where passwords are set / changed manually, requests for password changes should be authenticated by IT in-charge to ensure that the new password can only be passed to the genuine user

7.9. Staff Passwords

- 7.9.1 All staff users will be provided with a username and password by the In-charge of IT department, who / which will keep an up to date record of users and their usernames.
- 7.9.2 the password should be a minimum of 8 characters long and must include – uppercase character, lowercase character, number, special characters.
- 7.9.3 must not include proper names or any other personal information about the user that might be known by others.
- 7.9.4 temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on.
- 7.9.5 passwords shall not be displayed on screen and shall be securely hashed.
- 7.9.6 passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school.
- 7.9.7 staff are encouraged to change on a regular basis.

8. Education / Training / Awareness

Students will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Policy and Filtering Policy
- induction training
- staff meetings, briefings.

Parents will be informed of the school's filtering policy through the Acceptable Use Policy and through online safety awareness sessions/newsletter/website etc.

9. Strategies for Managing Unacceptable Use

In the event of a breach of this Acceptable Use Policy by a User, Delhi Private School may in its sole discretion manage the unacceptable use as per the following strategies.

- Actions will be taken as per the sanctions mentioned in ANNEXURE I of this policy
- The Online Safety Leader will investigate the concern provided by the teacher/student/parent.
- Take appropriate action as per the Ministry of Education- Behavior Management on Distance Learning 2020 Bylaws.
- Restrict or terminate a User's right to use the Network if necessary.
- Withdraw or remove any material uploaded by the user if it is in contravention of this Policy.
- Where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.

10. Monitoring and Review of the Policy

The implementation of the Online Safety Policy is the responsibility of each member of the school and will be monitored by the Online Safety Leader and the IT in-charge. The policy will be reviewed and evaluated annually or as per the requirements. On-going review and evaluation will take in cognizance of changing information and guidelines by the Ministry of Education (MOE). The policy will also be reviewed as necessary in the light of reviews of the incident logs, and evaluation within the framework of school planning.

As students are gradually being ushered back into the classroom, we must ensure they are protected from growing cybersecurity threats. DPS Ajman are committed to keep our students

and staff safe online. This means making sure all internet activity is appropriate, relevant to learning and doesn't open the doors for malware and other cyber-attacks.

DPS Ajman invested Sophos Firewall solution which is purpose-built for Education that delivers the key features as below:

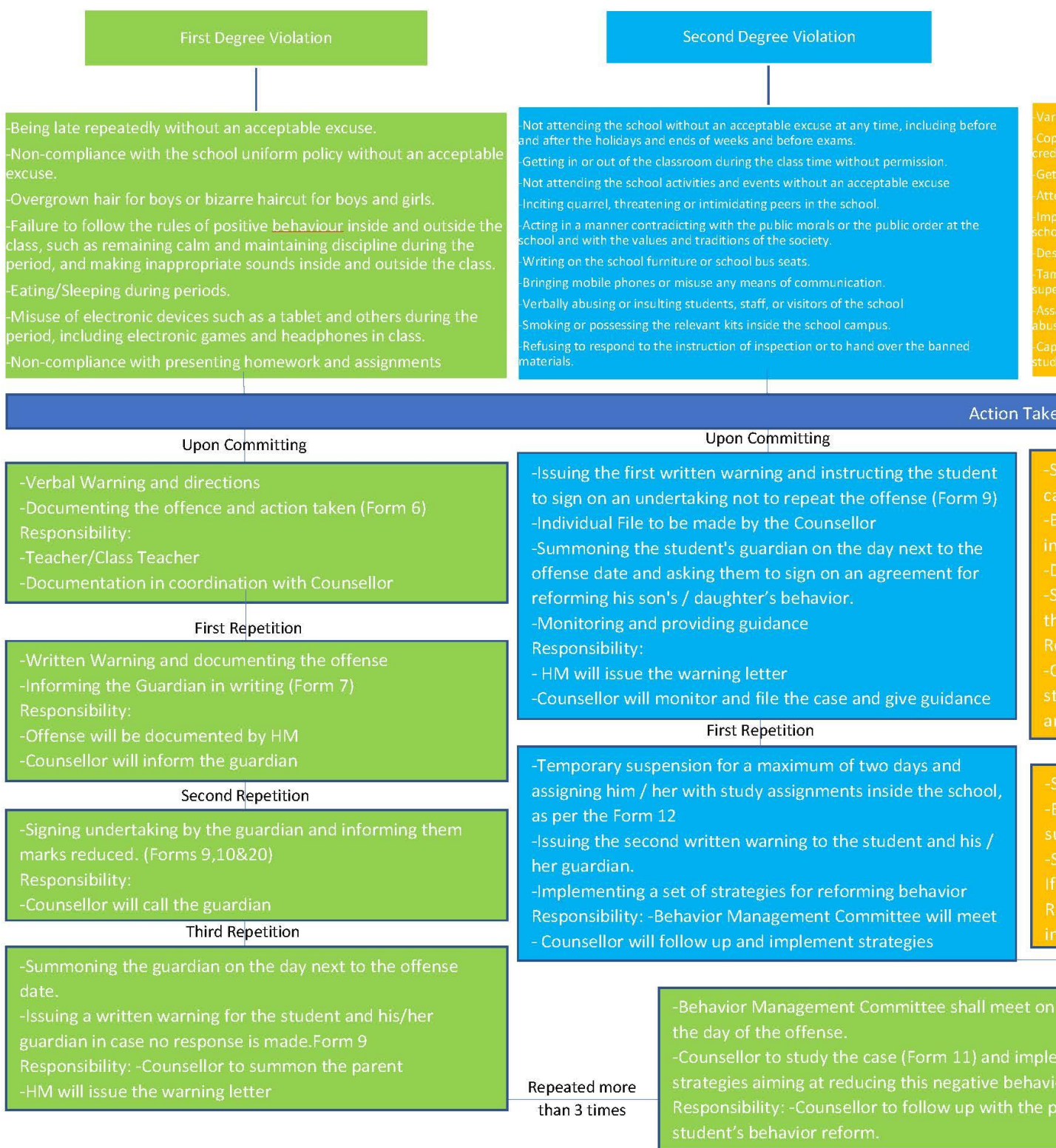
- Powerful web-filtering policy
- Child safety and compliance
- Context-aware keyword filtering



DELHI PRIVATE S

PB No: 21900, Al Tallah 2, Ajma
 Email: info@dpsajman.com, w

Sanctions for Concerns related to Unacceptable U





DELHI PRIVATE SCHOOL, A

Are you facing any kind of **cyberbullying/e-safety concern** Or you want to share a concern faced by **any other child** or **report an incident?**



Parents,
Concerned
Teacher,
e-COPS

Class Teacher,
Ms.Shafeena
(Cycle Head),
Secretary e-safety,
Secretary Cyber Club

**Ms. Shyama
(Supervisor)**
(personal
meeting or mail:
pr.supervisor@dpsajman.com or
call on
0555311442)

**Mr. Christy
(Online Safety
Leader)**
(personal meeting, mail
osl@dpsajman.com,
google form shared
through Google
Classroom, or call on
0543862341)

Principal
(personal meeting
or mail
principal@dpsajman.com)

**Primary Section
Grade 1-4**



DELHI PRIVATE SCHOOL, A

Are you facing any kind of **cyberbullying/e-safety concern** or you want to share a concern faced by **any other child** or **report an incident?**



Report
for everyone

Parents,
Concerned
Teacher,
e-cops

Class Teacher,
Ms. Manasa
(Cycle Head),
Secretary e-safety,
Secretary Cyber Club

**Ms. Anu
(Supervisor)**

(personal
meeting or mail:
sr.supervisor@d
psajman.com or
on 0506399529)

To Mr. Christy (OSL) or
Head or as per the flow
[click here](#) to re

**Grade 5-12
(Girls)**

**Mr. Christy
(Online Safety
Leader)**

(personal meeting, mail
osl@dpsajman.com,
google form shared
through Google
Classroom)

Principal

(personal meeting
or mail
principal@dpsajma
n.com)



DELHI PRIVATE SCHOOL, A

Are you facing any kind of **cyberbullying/e-safety concern** or you want to share a concern faced by **any other child** or **report an incident?**



Report
for everyone

Parents,
Concerned
Teacher,
e-cops

Class Teacher,
Ms. Gaina
(Cycle Head),
Secretary e-safety,
Secretary Cyber Club

**Ms. Khadija
(HM)**
personal meeting or
mail: hm
@dpsajman.com or
on 0502132054

To Mr. Christy (OSL) or
Head or as per the flow
[click here](#) to re

**Grade 5-12
(Boys)**

**Mr. Christy
(Online Safety
Leader)**

(personal meeting, mail
osl@dpsajman.com,
google form shared
through Google
Classroom on
0543862341)

Principal

(personal meeting
or mail
principal@dpsajma
n.com)