Cyber Policy

OBJECTIVE:

In today’s world, we are surrounded by electronic gadgets everywhere. As an educational institution, it is the school’s responsibility to provide Internet facilities and IT (Information Technology) devices / equipment which will benefit student learning outcomes, and the effective operation of the school.

However, these technologies (some provided partly or wholly by the school and some privately owned by staff, students and other members of the school community), can also facilitate anti-social, inappropriate, and even illegal material and activities. The school has the dual responsibility to maximize the benefits of these technologies, while at the same time to minimize and manage the risks.

Thus, we need to have in place rigorous and effective school Cyber Safety practices which are directed and guided by this Cyber policy.

VISION

To build a secured and resilient cyberspace for citizens.

NEED OF A CYBER POLICY

“To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.”

CYBER POLICY

This policy applies whenever students are using DAV Public School Information Technology equipment, services and/or resources, whether such equipment, service and/or resource is being used at school or home.

1. Students must not eat/drink near the IT devices.
2. They must respect school equipment and should not indulge in moving the IT equipment and/or cables.
3. Students must not cause damage to any equipment. If they spot any damage, they must inform the teacher immediately.
4. They must not use flash drives or any other external media(cell phone, hard disk, CD, camera etc.) for the purpose of
    1. Saving or transferring their work
    2. Installing new software

Without due permission from the computer faculty.

1. Viewing social media sites/Registering on any website/Downloading any material for use must be under the strict supervision of the teacher.
2. In the computer lab, Internet access is allowed only after permission from computer faculty and the computer faculty reserves the right to check IDs of the users.
3. Students are not allowed to bring equipment such as iPad, iPod, PSP, mobile phones etc. to the school. Any such equipment confiscated from the students will be kept with the school.
4. Students must report incidents of Cyber Bullying and misuse of IT resources to their teachers/parents immediately.

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 Cyber bullying 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.

"Cyber bullying won't stop if it's ignored – you can help by listening to your child and working with them to take control of the situation."

GUIDELINES TO USE THE INTERNET SAFELY

- Don't give out personal information such as your address or phone number.
- Don't share passwords, user names, account IDs or PINs with anyone besides your parents?
- Don't share other people's personal information or say things that might violate the safety or rights of others, even if you mean it as a "joke".
- Don't leave the ICT devices unattended.
- Don't open emails or attachments from people you don't know.
- Don't become online 'friends' with people you don't know.
- Never arrange to meet someone in person who you've met online.
- If anything you see or read online worries you, tell your parents/teachers about it.
- Never give out personal details in messenger or in personal profiles.
- Don't send pictures to strangers.
- Remember that people may not be who they say they are.
- Most reputable chat rooms allow you to block messages from a particular sender.
- Be careful about who you share photos with.
- Use social network's privacy settings so only your friends can see your stuff.
- What you do not do in real life, don't do on the Internet. This includes all kinds of cyber bulling using text, photos and videos.
- Posting embarrassing content or pictures on internet can lead to trouble.
- Download carefully.