POLICY TITLE: SAFE USE OF ELECTRONIC DEVICES – STUDENTS, STAFF AND SYSTEM ADMINISTRATOR
Published: 2017

Legislation:

- Copyright Act 1968
- Copyright Amendment (Digital Agenda) Act 2000
- Copyright Amendment (Moral Rights) Act 2000
- Education (Participation) Amendment Act 2009

Procedures:

- Acceptable Use of ICT Guidelines.
- Use of Third Party Web-based Educational Services Guidelines and Mandatory Procedures.

This policy provides a framework for school to support student use of Personal Electronic Devices (PEDs) at school.

1. Policy Statement

1.1. Jaypee Public School, Noida students are not allowed to bring **Personal Electronic Devices (PEDs)** at school but in exceptional case like assistance in project work or some competition, they need to take prior permission from the school.

1.2. The use of PEDs is to enhance and enrich personalized, student-centered learning but these should be used with adherence to the school policies.

1.3. There is no single PED endorsed for sole use in schools. Schools will consult with their communities about PED preference and usage, timing of the transition to the use of PEDs, which year groups will be participating and to ensure equity for all students.

1.4. The use of PEDs at schools will be governed by this policy.

1.5. Prior to bringing their own PEDs to schools, staffs, students and parents are required to be familiar with this policy and the ***Information Security Awareness materials for student, teachers, system administrators available at http://infosecawareness.in/.***

1.6. The ***Use of Third Party Web-based Education Services Guidelines and Mandatory Procedures*** document outlines the responsibilities of schools, staff, students and parents when accessing third party websites for educational use.

1.7. **On safety of children in the school bus,** to deal with unprecedented emergency, the mobile phone of basic model without internet facility and data storage will made available, as per the CBSE Circular No 8/2017/1217401 dated February 2, 2017.

2. Who does it apply to?

2.1. This policy applies to all school staff, all those enrolled to attend a school administered by members of the school community.

3. Context

3.1. Students will use ICT in a variety of ways including class work, homework, projects and assignments; as well as collaboration and communication with others (including - but not limited to - students, teachers, guest speakers, community members and international experts) across the ACT and around the world - sharing ideas, challenges, knowledge and information.

3.2. Effective use of ICT allows schools to strengthen communication with parents and carers, and streamline administrative processes.

4. Procedure

4.1. Information Security Awareness for Students

Some Golden Rules to follow when you're online:

- Don't give out personal information such as your address or phone number.
- Don't send pictures of yourself to anyone, especially indecent pictures.
- 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 whom you've met online.
- If anything you see or read online worries you, tell someone/inform your parents about it.

4.1.1. Using a Web Browser

Using the Web browser is easy; to do things online, but there can be some hidden dangers to you and your computer. These risks can include exposure of sensitive personal information and infection by malware, which includes viruses, spyware, and adware. Safe browsing means being aware of these online threats and taking the necessary precautions to avoid them.

Follow these guidelines to protect your personal information and your computer online.

- Install and maintain up to date anti-virus software on your computer or device.
- Keep your internet browser up-to-date
- Be alert to unusual computer activity or problems.
- Install and maintain a firewall on your computer.
- Use a modern browser with features such as a pop-up blocker.
- Avoid storing sensitive material indefinitely on your computer.
- Change your passwords often.
- Beware of links sent via instant messaging and e-mail attachments.

4.1.2. Making ‘friends’

We all know it's not healthy to spend hours and hours in front of a computer screen. But another problem with social networking is the pressure you can feel to make sure you have lots of ‘friends’. But here are some things to remember:

- Friendships made online are made by clicking a button rather than talking to people and sharing experiences.
- Being online ‘friends’ with someone is much less meaningful than face to face friendship.
- You can easily fall out with an online ‘friend’ because of a misunderstood comment.
- It is far easier, and healthier, to sort out arguments and problems when you can talk to someone face to face.

Tips to stay safe on social networking sites

- Make sure you're old enough to join.
- Maybe use a made up name or nickname on your profile.
- Do not make friends you don't already know personally.
- Maybe use an email address that does not include your name.
- Use the strongest privacy setting when you set up your profile. This means that only your friends will be able to view your information.
- Pictures and Videos can be shared very careful when uploading-even if you only share it with friends, it can easily be spread much further
- Be very careful about sharing content online - especially if it isn't yours to share. Illegal downloads definitely should be avoided.

4.1.3. Smart Phone Security

With modern smartphones we can do a wide range of tasks; everything from browsing the Internet and paying your bills to checking your bank statement and accessing work emails. Because smartphones are so advanced many of the security issues we’re exposed to through our computers now exist on our smartphones.

What risk does it pose?

- Device loss or theft. Losing a device to mishap or theft can cause lost productivity, data loss, and potential liability under data-protection laws.
- Loss of sensitive data. Many mobile devices may contain sensitive or confidential information, for example, personal photographs and videos, email messages, text messages and files.
- Unauthorised network penetration. Because many mobile devices provide a variety of network connectivity options, they could potentially be used to attack protected

corporate systems.

- Intercepted or corrupted data. With so many business transactions taking place over mobile devices, there is always a concern that critical data could be intercepted via tapped phone lines or intercepted microwave transmissions.
- Malicious software. Viruses, Trojan Horses, and Worms are familiar threats to mobile devices it has become a significant target.

How can we avoid it from happening?

- When choosing a mobile device, consider its security features and ensure they are enabled.
- Install and maintain an Anti-Virus application on your smart device.
- Do not follow links sent in suspicious email or text messages.
- Carefully consider what information you want stored on the device
  Be cautious when selecting and installing applications
- Avoid joining unknown Wi-Fi networks and using unsecured Wi-Fi hotspots.
- Disable interfaces that are not in use, such as Bluetooth, infrared, or Wi-Fi.
- Delete all information stored in a device prior to discarding it.

4.2. Information Security Awareness for Students

A teacher should be aware of the internet and its advantages and disadvantages. Creating cyber security Awareness is very much required for a teacher to impart the knowledge about pros and cons of internet usage and safety tips for online presence. In turn the Teacher should be aware of the cyber threats and how to safe guard himself and disseminate the knowledge to all students and parents. Cyber Awareness on this page are aimed at assisting teachers to understand and teach some of the issues about information security, cyber safety, cyber bullying and the Guidelines to be safe online.

4.3. Information Security Awareness for System/Network Admin

System Administrators are primarily responsible for keeping systems/computers/network devices to work smoothly and securely in any organization. Further they are also responsible for the continuous operations of the networks and computers to the end users for their business needs. It is very important to the System Administrator’s to keep the information as much securing the system and network devices in the organization.

By following simple practices/standards during their administrative functions, they can maintain the security of IT devices. The practices for security also help in reporting security incidents at an early stage and take corrective measures so that they can safe guard the business. As part of Awareness, ISEA Phase-II introduces best practices and guidelines for systems and network devices.

The system admin should have their own policy as per the organization policy:

- Because to maintain system intact as per the organization policy
- To give seamless support to the end users
- Every organization must have an overall policy that establishes the direction of the organization and its security mission as well as roles and responsibilities.
- There can also be system specific rules to address the policies for individual systems, network and application security.
- These policies should be included in the employee handbook and uploaded on a company intranet site.

Before keeping the system and network devices in the work place or in the existing network, it is very important to follow some of the best system/network practices

- Harden the Operating System before keeping into the network
- Harden the Integrated OS and its application's installed
- Have all the network architecture in one place
- Harden the network by using the vulnerability Assessment process for any open ports and any vulnerable applications
- Harden the Servers by running least services which is actually required
- Always have a knowledge update on the security loopholes of the systems and networks.
- Always provide the physical security to the internetworking devices attached to the network.
- Always Document the systems/Networks configurations and whenever any changes happen.
- Monitor Your Systems Periodically by downloading the system/network logs
- System Administrator and Network Admin need to educate users and help-desk personnel about basic security issues and practices to follow.

5. Definitions

5.1. ICT resources refer to the hardware, software, and services related to information and communication technologies (ICT).

5.2. A **parent** is a person with legal parental responsibility for the student. This includes caretakers and legal guardians.

5.3. PEDs or **Personal Electronic Devices** refers to (but is not limited to) workstations, laptops, tablet devices and smart phones which are owned by individual users and brought to the school.

5.4. Student(s) includes all those enrolled in school.

5.5. Third Party Web Services refers to external web services used in an educational capacity that are not hosted within the Directorate's environment.

5.6. **Users** refer to students, parents, guardians and community members that access the Directorate's ICT resources.

6. Legislation

6.1. The Education Act 2004 (ACT) allows for the exclusion of students from school activities if their actions compromise the good name of the school or the safety or wellbeing of other students. This includes online activities.

7. Policy Owner

7.1. Jaypee public School, Noida

7.2. For support in relation to this policy please contact the School's Chief Information Officer on ___________________.