IT Usage policy

VISION

Our vision is to be a globally renowned academia fostering excellence in future – ready robust pedagogy and profound learning environment to disseminate values of academics freedom and the spirit of collaboration and innovation. To develop an ethos of entrepreneurship and build ethical future enterprise leaders who add value to society, spearhead in nation building.

MISSION

Our mission is to impart quality value based education of international standard and focus on holistic development of the students imbibing skills for solving real life problems. Along with our clean and green campus – our infrastructure offers homey stay, hygienic food. It's our priority to engage all our staff from ground level to top management as a family to ensure that all students make a smooth transition to our institution and do not feel alone.

OBJECTIVES

1. **Promotion of value education and community service** : to impart values such as resilience, determination, confidence, and creative & critical thinking, to develop good social skills and the ability to form good relationships, to promote participation in community life and fulfilment of civic and social responsibility.

2. **Instilling cultural, linguistic diversity and heritage** : to instill the importance of inclusion within society of different groups and persons with different personal characteristics, the diversity of society, cultural knowledge, various languages, India's cultural values, history and its rich heritage, yoga, Ayurveda and holistic living, to implant cross cultural dexterity.

3. **Cognitive Acceleration Program** : To encourage schema (class preparedness), cognitive conflicts (make the children face challenges and to solve problems in collaboration), social learning, meta cognition (knowing about knowing), bridging (transferability of knowledge), teacher mediation to master learning.

4. **Internationalism and Entrepreneurship:** To promote global citizenship, globalization and sustainable future, physical & psychological health, inter personal skills to enhance employability skills.

5. **Nurturing Leaders:** To instill leadership qualities, to foster the physical, intellectual, technological, social, emotional, and artistic development of the students, develop self-discipline and personal responsibility, to promote creativity, effective communication, and critical thinking skills, to have a strong student leadership program with active involvement of students of all age groups.

6. **Multi literacy:** To develop the ability to interpret, identify, create and communicate meaning across a variety of visual, oral, musical and alphabetical forms of communication.

7. **Curriculum and learning atmosphere :** To build a curriculum leading to experiential learning and to have multiple curricula, to provide clear learning outcome, detailed instructions and assessment for all courses to ensure course mastery, student success, to offer a dynamic, interactive educational environment that engages students in the learning process, to promote inter-disciplinary learning, to review and update curriculum, instruction, and assessment in a regular cycle.

8. **Assessment practices:** To support every child's individual strength, Self-assessment, Peer assessment, learning how to give feedback.

9. **Teach less and learn more strategy:** To reduce lecturing from podium, to increase quality of education not quantity.

10. **Technology and digitalization:** To use technology to create effective modes and means of instruction and expand access to learning, to educate the students in futuristic technologies, to have robust digital infrastructure.

11. **Safe campus:** To be a residential school of international standard providing safety and security, in a healthy and hygienic atmosphere.

12. **Community partnership:** Cultivating the educational partnership among home, school, and community, nurturing a culture of collaboration, collegiality, and mutual respect

13. **Professional Development:** Implementing professional development for the staff that is essential for effective instruction and improved student learning.

14. CORE VALUES (SPIRIT OF PSSEMRS)

1. **Metacognition** –
    a) Knowing about knowing
    b) Learn until perfection is achieved.
2. **Growth mindset**
    a) Understand that we are continually learning
    b) Helping each other learn and succeed
    c) Healthy competition.
3. **Pursuit of excellence**
    a) Resilience in every action
    b) Greatest involvement to pioneer
    c) Act with responsibility and compassion
4. **Uncompromising integrity**
    a) Act with fairness
    b) Maintain transparency
    c) Unyielding integrity

IT Usage policy

This policy is designed to give all staff the information for the recognition and management of physical assets. The information provided will define assets and inventory items and detail the procedures for their management.

The Governing Body of the School is responsible for the proper management and security of the school premises and the custody and physical control of all other assets including machinery, furniture, equipment, stock and other assets such as cash.

The Stock Register

The School maintains a stock Register of items held by the school that the Governing Body deems to be valuable and/or subject to an insurance claim. Moveable assets must be recorded. Note that all information Technology (IT) equipment must be recorded.
The stock register should include the following information:

- Data of acquisition of asset
- Description of asset, including colour, a unique identification mark such as serial number and security making, where appropriate.
- For ICT/electrical equipment, a record of the model or other unique reference/security number
- Cost of the asset purchased
- Source of funding
- Location of the asset
- Details of the disposal of any assets, whether scrapped, sold, donated
- Details of the revaluation of an asset
- Items used by the school but owned by others (eg leased items) supported by a note of ownership Where possible, the stock Register should be held within the school's financial system, rather than as a hardcopy document.
    - A copy of the stock Register must be kept in a safe, fireproof place, and be available for inspection.
    - Acquisitions and disposals should be recorded on the register at the time of acquisition or disposal and reported to the governing Body.
    - The Governing Body must ensure that the stock register is kept-up-to-date and is reviewed at least once a year. The review must include the physical check of the assets and must be performed by someone other than the person maintaining the register. The stock register should be certified and dated on completion of the review. Typically asset review shall start on the 20th of March each year and be completed by 31st of March every year. The following format is followed –

Sl. No	Name of the Asset for stock verification	Location	Name of the reviewer	Date	Signature

-
    - The upkeep of the stock register can be particularly important for insurance reasons, as policies will often limit the insurance of equipment etc to those items present on the school stock register.
    - Register should be reconciled annually with the School's insurance Services records. Where the school participates in the insurance programme, the register submitted to the insurer should contain all audio/visual/ICT items.

Loaning Assets

An asset can be loaned to staff of the school must keep a log of such loans,the relevant paperwork must be completed. (Refer to system admin policy)

Disposing of Assets

- The Governing Body of the school may dispose of assets through sale, donation or scrapping.

- Assets that have been disposed of must be removed from the Asset Register, and the insurer notified.
- For every disposal, the Governing Body or the person who is maintaining the Asset Register must.
    - Record the reasons for the disposal
    - Be able to demonstrate that the assets are either obsolete or surplus to requirements
    - Facility manager is a single person responsible for disposing of assets, with prior approval from the Dean and the Chairman.
    - Any disposal of a capital asset must be made in accordance with the school's policy on purchasing and disposal.
    - The School must ensure that they adhere to the latest Legislation, which sets out the requirements for disposing of electrical/electronic equipment,
    - Before disposing of computer equipment, school must ensure compliance with Data Protection Act as passed by central and state governments from time to time by erasing all personal data from the hard disk. Note that merely deleting files may not physically remove the data, which could be restored using specialist products.
    - Ensure that any software products for which licences are maintained in – house are removed from the equipment prior to disposal.
    - Any member of staff who determines that an asset is surplus to requirement, or who is involved in the disposal, should never attempt to purchase it or take it for personal gain. There should be a clear separation of duties and the Dean and Chairman must approve all disposals.
    - Official receipts must be issued for income received for disposed assets. Money must be received and properly accounted for by someone who has not been involved in the disposal.
    - The income received from the sale of any asset must be treated as income in the school's budget.

Obsolete Assets

Assets are deemed obsolete if they have no resale value. The school may donate surplus, obsolete assets to the voluntary sector or scrap them only after the approval of the Chairman.

Surplus Assets

Where the possible sale value for an item or group of items exceeds a predetermined threshold value, the school should seek to dispose of them by quotation, competitive tender or public auction, unless approved by the Chairman to do otherwise.
The threshold value should be set by the Chairman.

Retention of Disposal Documentation

All documentation relating to the disposal of the asset must be retained for a period of three years after the disposal.

The following types of document should be retained:

- The Governing Body written record declaring the asset surplus, and instructions to the person appointed as responsible for the disposal
- The advertisement
- The offers made and the receipt.

Security – General

- The Governing Body is responsible for the security of the school's assets.
- It is responsibility of all Budget Holders to ensure that a yearly stock check is carried out at the end of financial year. Any missing items must be reported to the Governing Body.

Security measures include the following:

- Secure equipment and other assets by means of physical and other security devices (eg locked in cupboards)
- Authority to access these secured assets is documented through a below format right in the beginning of the financial year.

Sl. No	Date	Name of the Asset	Custodian Name	Signature

- All items in the Stock register should be permanently and visibly marked as the school's property.
- Maintain a record of any model or other unique reference/security number in the asset register.
- Clearly mark any portable equipment that is vulnerable to theft with the name of the school.
- Items which are easily portable and saleable (videos, televisions, computers, cameras, etc) must be security marked and kept securely locked away when not in use, particularly overnight, keep a separate record (in the Asset Register) of any model or other number unique to your machines.
- Items of school property should not be removed from the school premises without the appropriate delegated authority.
- Be aware that assets on loan for extended periods or to a single member of staff on a regular basis may be deemed a benefit-in-kind.
- Keep a record of all assets removed from the school premises.
- Update the record when the assets are returned.

Computer Security and Protection

School computer systems hold sensitive financial and personal data. School must therefore, take appropriate action to ensure that equipment and data is kept secure.

ICT Security Policy

Computer Usage Policy

The School provides access to various computer resources, including the school network, and the internet. These resources are available to facilitate the learning process in a supportive school environment and to provide quality learning outcomes for our students. The School encourages students to become familiar with the use of information technology in the achievement of learning outcomes and personal learning goals. As responsible member of the school community, it is expected that all students will follow and adhere to the guidelines established below. These guidelines are based on respect, common sense, school rules and procedures, as well as other state and central legislation. For the benefit of all users, students are expected to observe the following:

1. Use of Information Technology Equipment
    a. The school has endeavoured to ensure that all students' work can be saved, stored and accessed in a secure manner.
    b. It is expected that all students will respect the right of other students to use the network resources.
    c. It is expected that all students will respect the information technology equipment with which they have been provided, and realise that using this equipment is a privilege, not a right. This privilege can be withdrawn if necessary as set down in the student code of conduct and safe school policy.
    d. Access protocols include:
        i. Log in using your own appropriate ID. It is never acceptable to use someone else's ID or share your password with another person.
        ii. Use computers for the purpose directed by the teacher in charge. Students are not to play games or use other software unless the teacher has given specific permission for this.
        iii. Do not tamper with the computer system. It is unacceptable to seek access to restricted areas of the computer network.
        iv. Do not swap around any equipment. That is, no changing of keyboards, mice or other equipment from one computer to another.
        v. Report all equipment faults to the teacher immediately.
        vi. Computers are not to be used unless permission has been given by appropriate staff.
        vii. Passwords: (for computers with individual user log on) Keep your password secret. If you suspect that someone may know your password, see your class teacher to have it changed.

viii. It is unacceptable to gain, or attempt to gain, another person's password or personal information.

ix. It is the student's responsibility to remember that password. If a student forgets their password, he/she is to see the system administrator to have a new password provided.

x. In case of Bring your own devise situation, the student is expected to cooperate with the school to lock his/her devise for the use of educational purposes only. Violation will lead to actions as per discipline policy and such act is against the student code of conduct.

Printing

The school has provided printing facilities for students to obtain printouts of their work. Students are expected to use the printers for school purposes only and endeavour to keep paper wastage to a minimum. Before printing, always proofread, spell check, and print preview your document. When completely satisfied with the final product, print your document. Place unwanted printouts in the recycling box. Where possible, use duplex (i.e. double-sided) printing options.

Use of the Internet

What is the Internet?

The Internet is a world-wide network of individuals, groups, communities, and organizations linked via computer and telecommunication lines. In trying to visualise the Internet, people often describe it as a gigantic library, others an infinitely large encyclopaedia, while others as a jungle of intertwined information not a spider's web.

Why are educational institutions using the Internet?

Teachers and students are using the Internet to locate information, send electronic mail, browse documents or images from various sites such as universities, libraries and other organizations in and around the country. They are sharing or publishing information and ideas on topics of educational interest. Students will use the Internet for educational purposes in curriculum projects with the assistance and guidance of their teachers.

Educational institutions use the Internet for:

1. **Electronic mail** : Accessing information Electronic publishing Collaboration with others Curriculum projects Support and in-service training Technical support.
2. What about the availability of unacceptable material on the Internet? There has been a lot of media attention on the unacceptable materials found on the Internet. Given that there is no guaranteed means of preventing students' exposure of this material, other strategies must be adopted. This School has developed monitoring strategies, by providing appropriate levels of supervision to students using the Internet and checks of logs of sites accessed. The other part of our strategy is developing responsibility and awareness amongst teachers, parents and students of possible problems and the procedures for dealing with them.

What are the responsibilities of each member of the school community?

The Role of the School

The School undertakes a commitment to provide appropriate and financial resources to facilitate the successful incorporation of access to Information Communication Technology services throughout the curriculum in accordance with established school policies and procedures. In addition, the school will actively support the professional development of all staff to ensure the effective inclusion of information technologies, including the relevant information skills, into the school's curriculum.

The Role of the Staff within the School

The School expects that each staff member will aim to incorporate appropriate use of electronic information throughout the curriculum (as they would any other curriculum resource) and that teachers and staff will provide guidance and instructions to students in the appropriate use of such resources, Staff will facilitate student access to curriculum information resources appropriate to the individual student's instructional needs, learning styles, abilities and developmental levels.

The Role of Parents

Parents and carers are ultimately responsible for setting the standards that their children should follow when using media and information sources, and ensuring that these standards are met. This school expects that these standards will be in accordance with the School Mission Statement, Student Code of Conduct and other school policies including, but not limited to, the signed School Internet Access Agreement.

The Role of Students

Students are responsible for appropriate behaviour on the school computer network as detailed in the school's Student Code of Conduct relation to general school behaviour. They must comply with specific computer rules including those outlined specifically within the Computer Usage Policy and Internet Access Agreement. Communications on the information networks are public and users should not expect that files stored on school equipment will always be private. General school rules for student behaviour, conduct and standards will apply. Individual uses of the school networks are responsible for their behaviour and communications over these networks. It is presumed that students will comply with school standards and will honour the agreements they have signed.

Copyright

Students are expected to respect and adhere to the laws concerning copyright and other people's ideas. Students must have permission before copying files from another user. Copying files or ideas belonging to another user or author without their permission may constitute plagiarism or theft.

Breach of Rules

Breaches of this Policy and the Internet Access Agreement may result in

1. Students being excluded from using the school's computer equipment
2. Penalties and fine

3. Expulsion for repeating the offence
4. Any other disciplinary action as per the Student code of conduct and safe school policy.

Software

1. Install only authorized software in the school computers
2. Observe and respect license and copyright agreements
3. Avoid Coping, renaming, altering, examining, installing or deleting the files or programs of another person
4. Refrain from creating, disseminating, or running a self-replication program
5. Access or attempt to access a desktop, network, or host computer without having obtained the appropriate access log-in ID and pass- word is not permitted
6. Tampering with switch settings or hardware (including keyboards, monitors and mouse devices), or to move, reconfigure, and/or do any- thing that could damage the school's property is strictly prohibited

Shared Folders/ Network folders

1. Keep username and password confidential
2. Attempt to access the folders/files which you are not authorized to access will lead to lead to consequences
3. Do not delete , modify or duplicate unauthorized data
4. Do not try to change the access permissions of any folder

Smart Boards

1. Do seek IT team's assistance in installation of Smartboards, related hardware and software
2. Do allow free flow of information
3. Do save whatever you teach for further reference
4. Do explore interactive whiteboard features and share your discoveries with Peers frequently
5. Refrain from writing on the smartboard with the board markers
6. Avoid using it as a projector

School ERP

1. Provide your legal full name, a valid email address, and any other information requested in order to complete the account registration process, and keep them up -to -date if your circumstances change.
2. Maintain the security of your account and password
3. Observe proper security practices on your local computer
4. Keep copies of all of the information published to the Website relating to you
5. One person may not have more than one membership

Student Internet Access Agreement

Students are encouraged to become familiar with the use of information technology. This agreement must be signed by students and parents/guardians annually and returned to the School's office in order for access to the Internet through the School's computer network to be allowed. Parents/guardians are encouraged to contact the appropriate personnel at the School if they require more information about this form. Please note that it is considered that both parent and student have signed this document if you are signatory to our application of admission.

Student

I understand that the Internet can connect me to useful information. While I have access to the Internet, I will follow all rules as stated in the Computer Usage Policy.

I WILL:

- Only use the Internet for the purpose directed by the teacher.
- Use the Internet solely for educational purposes. .
- Respect the rights and privacy of other users.
- Browse reputable and credible sites only.

I WILL NOT:

- Reveal any private information such as another person's name, address or phone number.
- Attempt to retrieve, view or disseminate any obscene, offensive or illegal material.
- Send anonymous or falsely addressed electronic mail.
- Download or print information without permission from my teacher.
- Use chat channels
- Disclose my home address, telephone number or any credit card or pin number.
- Attempt to change or tamper with the computer network in any way.
- Use of the network for commercial, political, personal, or private gain is not encouraged
- Broadcasting unsolicited commercial e-mail ("spam") thereby creating excessive network traffic resulting in congestion is not encouraged
- Users are responsible at all time for using the Wi-Fi network in a manner that is ethical, legal, and not to the detriment of others
- Network services and wiring may not be modified or extended beyond the area of their intended use.
- If I accidentally come across something that is illegal, dangerous of offensive, I will Minimize my screen, and Immediately and quietly inform my teacher.

Declaration

I declare that I have read the Internet Usage, email, IT Usage Policies and I understand that if the School decides I have broken this agreement, I may be prevented from using the Internet, my device may be confiscated for a period of time. If the offence is repeated, I understand that the action according to the student code of conduct and other relevant policies of the school will be initiated against me.

Parent/Guardian

I understand that the Internet system can provide students with valuable learning experiences. I also understand that, although unlikely, it may give access to information that is illegal, dangerous or offensive. I accept that, whilst teachers will always exercise their duty of care, protection against exposure to harmful information must depend upon responsible use by the students.

I give permission for to use the Internet network. I understand that students who break the Computer Usage Policy and/or Internet Access Agreement may be prevented from using computers and/or have disciplinary action taken against them.

Employee Internet Access Agreement

This agreement must be signed by employees annually and returned to the School's office in order for access to the Internet through the School's computer network to be allowed. Employees can request additional information from the appropriate personnel at the School.

Please complete this section to indicate that you agree with the terms and conditions outlined in the Computer, E-mail, and Internet Policy in the Employee Handbook. Return this portion to your supervisor, who is required to maintain a copy on file. Your signature is required before access is granted.

I have read and hereby agree to comply with the Computer, E-mail, and Internet Policy:

Assessment, recording and reporting

Students ICT work is kept electronically, wherever possible. Each child also receives a termly report at the end of each term as well as an annual review at the end of the academic year. ICT and School Administration The administration ICT is overseen by the Head of Department-IT. Where possible Administration and Curriculum ICT are integrated to enable effective collection of student data; to reduce duplication of data; enable better analysis and monitoring of performance and support target setting. Good use of integrated ICT provides us with greater access to management information held by the School ERP Curricula requirements.

Resources & Action plan At PSSEMR School and College

1. All classrooms have a teacher's computers and smart class systems.
2. Three ICT labs with 20, 14 and 25 systems respectively.
3. All staff rooms with one computer system at-least
4. School main reception (1 system), CBSE reception (3 Systems), PUC reception (1 system)

5. Design lab (computer and workstations)

Most of the classrooms are equipped with interactive whiteboards. In the following years the school aims to have one on one laptops/ tablets for all students. Also the school will be adopting a pilot project of tabs starting July 2022.

Head of IT Department is responsible for:

- Meeting statutory ICT requirements.
- Presenting an Annual IT Budget to the Senior Management Team.
- Ensuring that there is an ICT policy and that it is implemented.
- Reviewing and updating the ICT policy with the Senior Management Team.
- Ensuring that the IT Administrator is effectively line managed and supported.
- Monitoring and evaluating the purchase of ICT equipment.
- Develop a whole school curriculum for ICT in collaboration with ICT facilitators.
- Ensure smooth working of IT facilities in collaboration with IT admin team
- Ensure that effective communication is facilitated among all stakeholders of the school.
- Continuously engage in implementing new technology that will enhance Student learning.
- Plan Strategy for access of resources.
- Manage Admin accounts for all channels of communication.
- Maintain relations with external agencies regarding the use of ICT.
- Liaison with other schools.

Administration(system Admin)- It is the responsibility of the IT administration includes but not limited to the given details below, the IT admin team must ensure –

- All systems are up and running at all times.
- Health check of systems is carried out on regular intervals
- The school network is up and running at all times.
- All have access to school internet through intranet and wifi access.
- All software are updated. Only licence copies are installed.
- Staff has User ID on the server and allocate working space for staff.
- Smooth working of Biometric and EPBX machines
- Anti Virus updates
- Regular maintenance of UPS, Network devices, Biometric machines, EPBX, Computers, Laptops, Printers, Xerox machines.
- Safety norms are met at all times.
- They must also - Maintain the School Email Portal
- Report any malicious activity on server, email and print servers
- Regularly update the school website
- Look into the service request from teachers regarding hardware or software problems.
- Recommend replacements of old machines
- Maintain inventory of all IT equipment
- Issue and return of IT equipment given to staff

ICT facilitators-

ICT facilitators are responsible for creating the detail curriculum for each grade and they must prepare the timeline of implementing these each year. They must ensure that the whole school curriculum is vertically and horizontally aligned. All ICT facilitators are required to equip students with ICT skills to be used with other subjects also, trans disciplinary units must be prepared in connection with other subject teachers. ICT facilitators are required to upgrade their skills by attending workshops and higher course to keep abreast with ever changing technology. The ICT facilitators are also required to conduct training sessions for staff on a regular basis to equip them with latest in technology. Sessions must be focused on helping the staff integrate technology effectively in their lessons. ICT facilitators also ensure that the students and staff are aware of cyber safety and ethical use of technology.

Teachers - It is the responsibility of every teacher to plan and teach appropriate ICT activities and support the ICT team in monitoring & recording student progress in ICT. All teachers must abide by the responsible internet usage in school and the rules. They must use the ICT across the curriculum and provide interactive resources to the students. The teachers should encourage and motivate students to use internet to enhance their learning. Developing their own capability to support their teaching and students' learning. Report faults to the It admin team.

User Policy and safety rules

Examples of unacceptable uses that are expressly prohibited include but are not limited to the following:

- Accessing Inappropriate Materials
- Accessing, submitting, posting, publishing, forwarding, downloading, scanning or displaying materials that are defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal;
- Illegal Activities - Using School Department computers, networks and Internet services for any illegal activity or activity that violates other School Department policies, procedures and/or school rules.
- Violating Copyrights - Copying or downloading copyrighted materials without the owner's permission.
- Plagiarism - Representing as one's own work any materials obtained on the Internet (such as term papers, articles, etc.). When Internet sources are used in student work, the author, publisher and web site must be identified.
- Copying or Installing Software – Copying, downloading or installing software through school’s internet without the expressed authorization of the computer system administrator.
- Non-School Related Uses – Using networks and Internet services for non school related purposes such as private financial gain, commercial, advertising or solicitation purposes, or for any other personal use.
- Misuse of Passwords and Unauthorized Access - Sharing passwords, using other users’ passwords and/or accessing other users’ accounts.
- Malicious Use or Vandalism - Any malicious use, disruption or harm to School Department computers, networks and Internet services, including but not limited to hacking activities, breaching of security features, and creating, uploading or spreading computer viruses.
- Unauthorized Access to Chat Rooms, Instant Messaging or Newsgroups - Accessing chat rooms, instant messaging or newsgroups without specific authorization from the supervising teacher.
- Negatively Impacting Network Capacity – Engaging in activities that cause unreasonable demand on network capacity or disruption of system operation including but not limited to downloading large files without permission from the computer system administrator
- Social Networking- Use of social networking sites is strictly prohibited in school. Students below age of 18 according to National Cyber law are not eligible to have a account on Facebook , Google + or any other social networking site. Creating a false electronic record is an offence under the Information Technology Act and the Indian Penal Code .Please refer to sections of IT Law for reference. We request parents to refrain their wards from having accounts at these sites.
- National Cyber Law - Computing, network, and Internet resources must not be used to knowingly violate the laws and regulations of the country or any other nation, or the laws and regulations of any state, city, province, or local jurisdiction in any material way.

- Ownership - Students have no right of ownership or expectation of personal privacy to their Internet usage, including personal computers or laptops while on the PSSEMR and College campus. It is possible to monitor network and Internet usage, and PSSEMR and College reserves the right to inspect any and all network traffic and files at any time. PSSEMR and College reserve the right, without notice, to limit or restrict any computer, network or Internet usage.
- Privacy Policy - No one may use PSSEMR and College facilities to monitor use of computing or network resources by any other individual, or perform any probing, scanning, "sniffing," or vulnerability testing, except as otherwise provided by PSSEMR and College policies or law
- Virus - No one may use PSSEMR and College computer, network, or Internet facilities to deliberately propagate any virus, worm, Trojan horse, trap-door, or back-door program code or knowingly disable or overload any computer system, network, or to circumvent any system intended to protect the privacy or security of another user.
- Violating Filtration - No one may install, remove, or otherwise modify any software for the purpose of bypassing, avoiding, or defeating any filtering, monitoring, or other security measures PSSEMR and College may have in place, except as otherwise provided by PSSEMR and College policies

MANDATORY GUIDELINES

- Laptop is to be used for only academic purpose under supervision of dorm parents/ Teachers at designated locations.
- The laptops should not have any objectionable data at any point of time in it. (Videos other than related to academics, songs and movies, songs are not to be stored in any format.)
- The school has full authority to check any student's laptops at any point of time in his/her presence/absence.
- The school does not take any responsibility for the authenticity of software installed on laptops. All the software should be licensed.
- The laptops should be used during specified time as decided by dorm incharge/ Teachers only.
- The school's WIFI connection will be allowed only after the written permission from Principal, However, if sanctioned, the net must only be used for academic/research purpose. Downloading of any other material is strictly prohibited.
- Any student found accessing any restricted site which is not meant for him / her will be penalized and the same may lead to the school authority confiscating his / her laptop.
- The students are solely responsible for his/ her laptops.
- The school authority has full rights to make any change in the laptops for academic purpose.
- Any chat applet, messenger and social networking sites are strictly not allowed.
- Students can check their e-mails only during time decided by dorm parent.

- Headphones, Earphones, Gaming device and any similar kind of device are not allowed in the academic block.
- Students need to deposit their hard disks or pen drives with Grade Tutors and use only when required under supervision.
- The school authority has full rights to check any portable storage device of the students.
- The student's laptop should not have games and movies stored in it. Only videos related to academics should be stored. The laptop should also not have personal photos and videos in it which might be objectionable. Students willing to keep photos and videos must get them approved by IT department.
- The school has full authority to check any student's laptops at any point of time in his/her presence/absence.
- The school does not take any responsibility for the authenticity of software installed on laptops. All the software should be licensed.
- The laptops should be used during specified time as decided by wardens/ Teachers only.
- The students are solely responsible for his/ her laptops.
- The school authority has full rights to make any change in the laptops for academic purpose.
- Any chat applet, messenger and social networking sites are strictly not allowed.
- Students can check their e-mails only during time decided by wardens.
- Headphones, Earphones, Gaming device and any similar kind of device are not allowed in the academic block.
- Students need to deposit their pen drives with wardens and use only when required under supervision.
- The school authority has full rights to check any portable storage device of the students.

PSSEMR and College reserves the rights to confiscate the laptop in case the above points are violated. (Students and parents to sign the Agreement on page # after reading the policy) Student must not

1. Change the IP or any other configuration related to use of PSSEMR and College computers
2. Knowingly infringe copyright.
3. Download programs or games. (Except for Anti-Virus updates) Infractions of these policies constitute misuse of PSSEMR and College assets and therefore are considered violations of PSSEMR and College Code of Conduct and may result in disciplinary actions sanctioned under relevant provisions of PSSEMR and College Rules and Regulations

Protecting Hardware

The main dangers to hardware are:

- Loss through theft
- Damage (accidental or otherwise)

To minimise the danger of loss or damage, the machines should be:

- Labelled with a unique asset number
- Entered onto the school's stock register with their serial numbers
- Correctly positioned (i.e., towers not laid on their sides)

- If possible the machines should also benot visible from outside the building or to the public generally
- Kept in a locked room when not in use, particularly overnight where possible, secured to furniture llabelled, marked with indelible pen or have the name of the school soldered onto the case.

To minimise damage and the chances of the machines being damaged all users should:

- Refrain from eating or drinking whilst working on the machines.
- Never move or attempt to clean a machine without first obtaining the IT coordinator's advice
- Ensure any loose cabling into the machine is no danger of being stood on or tripped over by staff
- Know who to contact in the event of a breakdown of the machine
- Laptops other easily portable equipment are particularly vulnerable to theft and damage. They should be kept in a locked cupboard when not in use and carefully protected when taken outside the office.
- File servers must be kept in secure rooms, with access limited only to authorised individuals.

Protecting Software

The main danger to software are:

- Unauthorized access to data
- Accidental loss of data by the user or because of machine failure
- Corruption of data by computer viruses

To minimise the danger of unauthorised access, users should ensure that:

- The system is returned to the password screen when leaving the office
- The machine is switched off when not in use
- Only authorised staff should have access to computer hardware and software for the school management.
- Passwords should be used to stop unauthorised access to information.
- Procedures should also exist for a new password to be issued to new staff, and withdrawn when staff leave.

Passwords should have,

- At least six character long and preferably contain a number
- Changed regularly (every 90 days) and as soon as a user leaves
- Not shared between users
- Not written down
- Not obvious (such as the user's telephone number)

- ✓ All financial data should be backed up every day.
- ✓ The following precautions should be taken to minimise any loss of data caused by machine failure or user error. (When PCs are networked and data is stored to a server, these functions should be carried out by the system Administrator)
    - o Give all proper written instructions or how to use the system.
    - o Back up all data regularly (ie files created by the user such as word processor documents or spreadsheet files). It is recommended that be backed up after 8 hours' work on the machine
    - o If possible, keep at least three generations of back – up (ie the previous three back – ups). Back – up cycles should be taken daily, weekly and monthly
    - o Maintain a back-up of all operating software (such as Windows)
    - o Store all back-up away from the vicinity of the machines in a fireproof, locked cabinet or safe-preferably off-site
    - o Ensure that there is adequate hardware maintenance cover for critical equipment
- ✓ To minimise the danger of data corruption by viruses and an-antivirus solution must be implemented for all networked PCs and servers. There is a continuing threat from previously undetected viruses, so staff should take the following precautions:
    - o Never load software without the school's IT co-ordinator's approval, including software from the internet.
    - o Never load any disks/CDs/pen drives sent unexpectedly through the post (for example, demonstration or customer research software)
    - o Strictly control the transfer of software and data from one machine to another
    - o Never make unauthorised copies of any software
    - o Ensure virus-checking software is installed on all computers, and regularly updated

Computer Printouts

Employees must not release information or computer data, particularly that of a personal or sensitive nature, to unauthorised persons.
Take care to prevent inadvertent disclosure of information, eg: by ensuring that paper is suitably filed and disposed of securely.
Confidential waste must be shredded.

IT admin team must ensure

- All systems are up and running at all times
- Health check of systems is carried out on regular intervals
- The school network is up and running at all times
- All have access to school internet through intranet and wifi access.
- All software are updated. Only license copies are installed
- Staff has User-ID on the server and allocate working space for staff.
- Smooth working of Biometric and EPBX(intercoms) machines
- Anti Virus updates

- Regular maintenance of UPS, Network devices, Biometric machines, EPBX, Computers, Laptops, Printers, Xerox machines.
- Safety norms are met at all times.
  They must also
- Maintain the School Email Portal
- Report any malicious activity on server, email and print servers
- Regularly update the school website
- Look into the service request from teachers regarding hardware or softwareproblems.
- Recommend replacements of old machines
- Maintain inventory of all IT equipment
- Issue and return of IT equipment given to staff.

Email Etiquette

- **Use the subject line to indicate the content of the email.** A subject line such as "Hey" does not provide insight into the content of the email and does not give the recipient a reason to read it.
- **Be concise.** Limit your email to one topic per message. Keep the email short, perhaps what can be read on a typical computer screen without requiring the reader to scroll down. Do not use bureaucratic language.
- **Be careful about using the *Reply All* feature.** When a message has been sent to multiple recipients, your response may be relevant to only the original sender, not to the entire recipient list. Do not clog the other recipients' inboxes with messages they do not need.
- **Include your contact information.** Many email programs allow you to include a signature, something which includes your full name, the name of your company, your phone number, and your mailing address.
- **The tone you think you're using in your writing may not be what the reader perceives.** Choose your words carefully, and avoid typing in all capital letters. Jokes and sarcastic comments may be interpreted differently than intended. Using all capital letters is the email equivalent of shouting. You may choose to use an emoticon (such as a smiley face) but remember that emoticons look unprofessional and do not take away the sting of a hurtful message.
- **Spelling and grammar count.** Your email presents you (and possibly your company) to your reader, so present yourself well through your writing.
- **Do not write in CAPITALS.** WRITING IN ALL CAPITALS SEEMS AS IF YOU ARE SHOUTING. It might get an unwanted response and come across as rude or aggressive.
- **Pick up the phone, or walk down the hall.** Some topics are better expressed in person or verbally than through an email. Anything that's personal, sad, or shocking is better discussed in person than through email.
- **Email is not private.** Whatever you write in an email can be forwarded to others. According to Laura Stack, anything sent over email at work is considered company property and "can be retrieved, examined, and used in a court of law."
- **Wait.** It's possible that you misunderstood an email you received, and your gut reaction might be to fire back something snappy. Remember that "the pushing of the **Send** button lasts a moment; its effects can last a lifetime."

- **Fill in the recipient box last.** Few things are as embarrassing as sending a message to an unintended recipient or hitting the Send button before you're finished writing.
- Never use BCC, never break the loop (CC, use reply all if you find addresses in CC)
- Do not propagate emails to which you are unintended recipient.

Footer and disclaimer

The information transmitted by this email is intended only for the person or entity to which it is addressed. This email may contain proprietary, business-confidential, and/or privileged material. If you are not the intended recipient of this message, be aware that any use, review, retransmission, distribution, reproduction or any action taken in reliance upon this message is strictly prohibited. If you received this in error, please contact the sender and delete the material from all computers.

This email may contain viruses that could infect your computer. We strongly recommend using a malware scanner to check the contents of this email and its attachments, if there are any. Since emails can be lost, intercepted, or corrupted, PSSEMR School & PU College accept no liability for damages caused by viruses transmitted via this email.

No employee or agent is authorized to conclude any binding agreement on behalf of PSSEMR School & PU College with another party by email without specific confirmation.

All views and opinions expressed in this email message are the personal opinions of the author and do not represent those of PSSEMR School & PU College. No liability can be held for any damages, however, caused, to any recipients of this message.

If you received this email in error, please notify us immediately by sending an e-mail to dean@pssemrschool.com or networkadmin@pssemrschool.com or by calling +91 8192 208432.

PSSEMR School & PU College is compliant with the privacy policy and Data Protection Regulation and various IT Acts of Government of India and other statutory local/state/district bodies. We are committed to guaranteeing the security and protection of the private information that we process. Any grievance may be reported to dean@pssemrschool.com or networkadmin@pssemrschool.com or by calling +91 8192 208432.

The following documents are adjutant to this policy

1) Stock register
2) Stock verification register
3) Stock issue register
4) Stock security custodian allotment report
5) IT asset allocation register
6) IT IP address register
7) Inventory label

This policy will be reviewed as per the review policy.