JSS PRIVATE SCHOOL

JSS

SEEK - LEARN - EXCEL

Information and Communication Technology (ICT) Policy

Reviewed on September 2016

PRINCIPAL

Introduction

The use of digital technologies at JSS Private School is to enhance the learning process in a supportive school environment. The school is committed to encourage and teach the positive use of digital technologies and promotes safe and responsible online behavior.

Objective

Objective for effective use of ICTs in education necessitates understanding the potential of technology to meet different educational objectives.

Main objectives are:

- Expanding access to all levels of education.
- Improving the quality of education.
- Facilitating non-formal education.
- Support individualized learning.
- Support collaborative and co-operative learning.
- Encourage flexibility, openness and awareness of changes and developments in ICT.
- Develop pupils' communication skills using Language lab.
- Develop understanding of cause and effect.
- Provide ongoing training opportunities and support for all staff.

Information Technology

This policy set forth standards for responsible and acceptable use of school information technology (IT) resources. These resources include computer systems, computer labs, applications, projectors, projector accessories, networks, software, and files. IT resources are provided to support the academic, research, instructional, and administrative objectives of the school. These resources are extended for the sole use of school faculty, staff, students, and all other authorized guests to accomplish tasks related to the status of that individual at the school.

2.0 Hardware Devices

2.1 Desktop PC

The aim is to use IT tools and information sources to analyze, process and present information to our pupil, parent, staff and management.

- User Account & password are maintained for Teacher's and Student separately.
- The teachers are advised to safeguard their password. For example, individuals should not write down or store the password on paper or on a computer system where others might acquire it. The teachers are responsible for the data stored in any of the systems in the school premises.
- The teachers are not advised to save any of the important files such as Question papers and internal marks, etc in the school lab machines as these machines are cleared periodically in every academic year by the IT resources.

- No staff or student is authorized to delete any of files from the school desktops / laptops.
- The staff and the students have to reach out to the IT resources in case of any new installation of non-standard software to be installed in any of the school Desktops or Laptops. Server admin user credentials are used only by IT resources for installation of software for academic purpose.
- All the school provided desktops are with Anti-Virus protected.
- Any hardware damage has to be immediately reported to the IT resources for investigation and replacement process.
- All hardware's used on school-owned computers will be purchased through appropriate procedures.
- If the device is lost or stolen, the incident must be reported immediately to their respective department head and a police report be made.

2.2 Laptop

- Laptops are given from school, only to selective staffs based on their work requirement.
- Using the school IT resources for commercial or profit-making purposes or to represent the interests of groups unaffiliated with the school or unassociated with the normal professional activities of faculty, staff, or students without written authorization from the School.
- If the device is lost or stolen, the incident must be reported immediately to their respective department head and a police report be made.

2.3 Mobile devices

Staffs may use approved personally owned and corporate owned mobile devices to access their emails using the approved corporate wireless network, as necessary in the course of their normal business routines in support of the schools objectives and goals.

User agrees to a general code of conduct that recognizes the need to protect confidential data that is stored on, or accessed using, a mobile device. This code of conduct includes but is not limited to:

- Doing what is necessary to ensure the adequate physical security of the device
- Maintaining the software configuration of the device – both the operating system and the applications installed.
- Preventing the storage of sensitive company data in unapproved applications on the device.
- Ensuring the device's security controls are not subverted via hacks, jailbreaks, security software changes and/or security setting changes
- Reporting a lost or stolen device immediately

2.4 Mobile Tabs

School owned devices like telephones and tablet devices are centrally managed by IT Services.

- Installation or upgrades of software's are done by the vendor or IT services.
- The academic content is provided by the vendor Ignitor.
- Specifically, the user is responsible for reporting lost or stolen device immediately to the admin officer.

- The user is responsible for securing their device to prevent sensitive data from being lost or compromised and to prevent viruses from being spread.
- Removal of security controls is prohibited.
- User is forbidden from copying sensitive data from email, calendar and contact applications to other applications on the device or to an unregistered personally owned device.
- If the device is lost or stolen, the incident must be reported immediately to their respective department head and a police report be made.
- Tablets must be stored in the trolleys and plugged in so that they can recharge. (This is the responsibility of the teacher)
- Tablets must NOT be placed on the floor. Must be on a hard surface e.g. table/ chair / lap etc.
- Water bottles, liquids and food items must be taken away from areas where computers / laptops / tablets are being used.
- It is the teacher's responsibility to take the tablet to either the next classroom or return to the resource room.
- The tablets and trolleys must be returned to the pod resource room at the end of the day to be plugged in and recharged.
- After each session teachers must check that all laptops / tablets are in the correct sleeve, in the correct drawer on the trolley and are plugged in.
- All drawers on the trolleys should are labeled so that tabs can be placed in their correct drawer.
- It is the duty of staff members to report any problems with tablets to the next teacher.
- This equipment is very delicate and needs to be handled with extreme care (in particular the cords and plugs.)
- Any changes to system settings are to be done only by the IT service.
- Damaging, disabling, or otherwise harming the operation of computers is forbidden.
- Never deliberately install and use software illegally or install any malicious code on school ICT resources. All software and hardware that needs to be installed and used must be approved by the IT co-ordinator.

3.0 SOFTWARE USAGE POLICY

3.1 Software Use

- Software will be used only in accordance with its license agreement. Unless otherwise provided in the license, any duplication of copyrighted software, except for backup and archival purposes by the software manager or designated department, is a violation of copyright law. In addition to violating copyright law, unauthorized duplication of software is contrary to (organization's) standards of conduct.
- The following points are to be followed to comply with software license agreements:
- All users must use all software in accordance with license agreements and the (organization's) software policy. All users acknowledge that they do not own this software

or its related documentation, and, that unless expressly authorized by the software publisher, may not make additional copies except for archival purposes.

- (Organization) will not tolerate the use of any unauthorized copies of software or fonts in our organization. Users must not condone illegal copying of software under any circumstances. Anyone who makes, uses, or otherwise acquires unauthorized software will be appropriately disciplined.
- All software's used on school-owned computers will be purchased through appropriate procedures.

3.2 Authorized Software

Only software authorized by school may be purchased, installed, or used on school issued computers.

Personal software, or software that an employee has acquired for non-business purposes, may not be installed on school issued computers. The only software permitted for installation on school computers is authorized software for which the school has been granted a license.

3.3 Software Purchases

Only software applications that are "authorized" by the school may be purchased by the staff. If you wish to purchase an authorized application, the following procedures must be adhered to:

1. Requirement from the respective department with the quotation should be submitted to Finance officer.
2. A copy of the software license must be provided to School for completion of registration and inventory requirements.
3. Licenses must be registered in the name of School Name and not in the name of an individual end-user.

3.4 Computer virus protection

We have virus protection software on all computers. Pupils generally store their work on the hard drive, but some class disks are also used. Pupils are not allowed to take these class disks homes, to reduce the risk of virus infection. However, some pupils may do work at home and wish to continue in school. These disks must be checked on a protected computer first. We will review this situation as home/school use increases.
All computers used for administrative purposes have anti-virus software installed as recommended and in accordance with the Schools IT Support Service.

We will ensure that we use an educational Internet Service Provider (ISP) with a filtering service. We will have an appropriate use policy in place, based on the school guidance.

3.5 Retirement or Transfer of Licenses

The following rules apply when a license or licenses are replaced by newer versions

- Licenses may not be uninstalled from one user's machine and re-installed on another user's machine.

- All software and documentation for releases or versions that have been replaced by newer versions are to be returned promptly to IT service.
- All software and documentation for those products no longer required should be returned promptly to IT service and the software must be uninstalled promptly from the computer by the IT service.
- No Software CD or documentation can be taken home.
- In most cases, software licenses are *not* transferable without prior authorization from the vendor. This is especially important as it relates to the disposition of previous releases and the disposition of software licenses that have been upgraded. For example, it is almost always a violation of the license agreement to give anyone an older version of Microsoft Windows after receiving a Microsoft Windows upgrade. Even if a new license (not an upgrade) has been obtained, it may be *still* be a violation of the license agreement to give the old copy to another person. Under some conditions, school may have rights to transfer software from one user to another. IT service will review license agreements and limitations for each software product, and if appropriate, authorize acceptable transfers of licenses.

3.6 Computer Reassignment

The following rules apply when a computer is being transferred from one user to another:

- The computer reassignment must be authorized by the Supervisor / Principal.
- The intention to transfer the computer must be reported to Supervisor / Principal at least 72 hours in advance to allow for proper procedure.
- If, after the transfer, both users are using the software, an additional license must be obtained according to the guidelines specified above.

3.7 Outlook

- All jsspsdubai.com user accounts that are used in school, will be maintained by the IT resources.
- Backup is taken by the IT resources in case of change in machine for any user.
- Outlook will be setup by the IT resources in the school provided computers or laptops.
- Office email account cannot be setup in personal computers or laptops. Whereas webmail can be used to access office emails.

4.0 ICT Policy

4.1 Student ICT Policy

- Students will access the Internet with the supervision of a teacher in the same manner as any other learning activity.
- Students to protect work by keeping their personal passwords private.
- The school reserves the right to examine all the data downloaded from the Internet to ensure all users are in compliance with our policy. This includes the use of USB sticks to store data. Data stored on USB sticks will be strictly for school related tasks.
- It is unacceptable to gain, or to attempt to gain another user's ID, password or personal information. A breach of this condition will result in immediate suspension of privileges.
- All students assume full liability, legal or otherwise for their actions while online. This includes online communication via sites, email and blogging. Email is not private so

messages that may be embarrassing, confidential, harassing, inflammatory or annoying must be avoided.

- Sending any personal information (full name, address, phone numbers, etc.) via email, blogging or internet is strictly forbidden.
- The school will not be liable for the inappropriate actions of users. The malicious attempt to harm, destroy the data of another user (vandalism) including the creation of or the uploading of viruses, shall result in the cancellation of privileges.
- Deliberate damage to Computers, Laptops, Learn pads, iPads, Digital cameras, Scanners, Printers and Interactive whiteboards shall result in the cancellation of privileges.
- Willful damage or deliberate tampering with network servers and data shall result in the cancellation of privileges.
- Students are encouraged to access information that will enhance the learning programs and policies of Emerson. At all times users are bound by the laws of copyright and plagiarism.
- The school does not accept responsibility if the ICT skills acquired at school are used for misconduct or to access inappropriate material outside the school setting.
- The Student Technology Agreement will be incorporated in the KHDA Parent School contract.
- To teach students to respect copyright and intellectual property.

4.2 Teachers ICT Policy

- All Data is stored in accordance with provision of the Data Protection.
- Use of someone else's personal logon/name or password is forbidden.
- To protect the ICT network, security on the computers must not be breached or settings on computers altered in any way.
- Students may not examine copy, alter, rename, or delete the files or programs of another student.
- System administrators may, as a requirement of system maintenance, delete files that are determined to be non-essential.
- Only relevant information and photographs of students will be used on the School website and for promotional material.
- All members of staff are offered training to improve their ICT capability and have a responsibility to keep abreast of developments in ICT.
- The IT Technician can be contacted to request additional support and training in the use of ICT.
- There is continuous attention to improve the quality of staff computers throughout the school subject to budgetary control.

Internet

- Social network Facebook.com is blocked in the school.
- Use of the Internet is for study or for school authorized/supervised activities only.
- Use of ICT resources must not be used for personal profit.
- Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- All measures have been put in place to protect vulnerable children from inappropriate approaches and from making inappropriate personal disclosures over the school network.
- "Chat" activities are banned.

- Respect the work and ownership rights of people outside the school as well as other students or staff. This includes abiding by copyright laws.
- Games may not be downloaded or played on any School ICT equipment.
- All Internet use on ICT resources is monitored on an on-going basis.
- Students need to be aware that e-mails sent and received as part of classroom activity are subject to monitoring.
- Parents must understand that their child may encounter material that they consider inappropriate (i.e. Vulgar Jokes, statements of belief that some may consider immoral, pornography, etc.,).
- The student is responsible for not pursuing material that could be considered offensive.

Prohibited Conduct

The following provisions describe conduct prohibited under this policy:

- Altering system software or hardware configurations without authorization; disrupting or interfering with the delivery or administration of IT resources.
- Attempting to access or accessing another's accounts, private files, email messages, or intercepting network communication without the owner's permission except as appropriate to your job duties and in accordance with legitimate university purposes.
- Misrepresenting oneself as another individual in electronic communication.
- Installing, copying, distributing, or using digital content (including software, music, text, images, and video) in violation of copyright and/or software agreements or applicable federal and state law.
- Facilitating access to School IT resources by unauthorized users.
- Exposing sensitive or confidential information or disclosing any electronic information that one does not have the authority to disclose.
- Knowingly using IT resources for illegal activities. Criminal or illegal use may include obscenity, child pornography, threats, harassment, copyright infringement, university trademark infringement, defamation, theft, identity theft, and unauthorized access.

4.4 ACCEPTABLE USE OF TECHNOLOGY AUP

JSS PS ACCEPTABLE USE OF TECHNOLOGY (AUP)

JSS PS students are expected to use technology in a respectful, responsible and safe manner following the guidelines below:

RESPECTFUL

Be courteous and ethical in all communications (email, social networking, etc...)
For example:

- When creating, publishing, posting or sending information in a private or public matter avoid profane language or bullying.
- Respect others' privacy, For example:
  - Only access personal files, folders or accounts of others with their permission.
- Respect others' ownership of property For example:
  - Ask permission before using the personal property of others (laptops, tablets etc.…).
  - Avoid eating or drinking near your devices or those of your friends and the school.
- Know where your devices are at all times.

- Respect others' ownership of information (Copyright), For example:
    - Taking someone else's work without giving them credit is plagiarism; you must properly cite all sources in your work.
- Respect your teachers and the learning environment of others, For example:
    - Students must comply with any teacher's request to shut down the device or close the screen.
    - Devices should be kept on silent or with the volume muted unless otherwise instructed by the teacher.

SAFE

Never share your passwords or personal information with anyone For example:

- Ask for teacher or parent permission before posting personal information online (personal information includes your full name, address, phone number, etc.).
- Ask permission of a teacher before downloading or installing any applications over the school network
- Notify a teacher if there are actions that do not follow the rules or seem unsafe

RESPONSIBLE

Ensure your usage of any technology devices is in line with school curriculum and approved sources
For example:

- During classroom instruction time, technology devices should only be used for class related projects and activities approved by the teacher.
- Only use websites that are allowed at that time by teachers.

Ensure that all personal and school property is used in the way that it was intended
For example:

- Only use the school network for school related activities.Use of 3G & 4G wireless connections is not allowed.
- Act responsibly when using personal or school hardware, software and the school network.

The use of personal devices to support educational goals is a privilege. Teachers and administrators have the right to see what the students are doing on the devices at all times. The school has the right to collect and examine a device if at any time it is used inappropriately or if the IT team suspects a virus that may be affecting the school network. Any use of technology that does not fit within these guidelines, as determined by a teacher or administrator, will result in disciplinary action.

BREACH OF POLICY

- If a student uses a phone during class in a manner that does not follow these guidelines, the phone will be confiscated and returned to the student at the end of class.

- If a student repeatedly uses a phone in a manner that does not follow these guidelines (determined by the teacher or administrator), the phone will be confiscated and the student or parent will be able to pick it up at the end of the school day from the assistant principal's office.

At the beginning of each new school year, students need to read, agree, and electronically sign the school AUP (Form 1)

(Form 1) PERMISSION FORM

Any parent must read and sign this agreement and submit to the administration upon registering their children at JSS PS.
1. The student takes full responsibility for his or her device and keeps it with himself or herself at all times. The school is not responsible for the security of the device.
2. The student is responsible for the proper care of their personal device, including any costs of repair, replacement or any modifications needed to use the device at school.
3. The school reserves the right to inspect a student's personal device if there is reason to believe that the student has violated school policies, administrative procedures, school rules or has engaged in other misconduct while using their personal device.
4. Violations of any school policies, administrative procedures or school rules involving a student's personally owned device may result in the loss of use of the device in school and/or disciplinary action.
5. The student must comply with teachers' request to shut down the computer or close the screen.
6. The student may not use the devices to record, transmit or post photos or video of a person or persons on campus. Nor can any images or video recorded at school be transmitted or posted at any time without the express permission of a teacher.
7. The student should only use their device to access relevant files.
8. The student will use the school's secured wireless network. Use of 3G & 4G wireless connections is not allowed.

SIGN AND RETURN TO SCHOOL ADMINISTRATION.
Student's name ________________________
Parent's name ____
I understand and will abide by the above policy and guidelines. I further understand that any violation of the above may result in the loss of network and/or device privileges as well as other disciplinary action.
As a parent I understand that my child will be responsible for abiding by the above policy and guidelines. I have read and discussed them with her/him and they understand the responsibility they have in the use of their personal device.
Parent's Signature _________________________
Date ________________________