
# Information and Communication Technology (ICT) & Cyber Safety Policy

*Reviewed on September 2023.*

## JSSPS Vision Statement on Wellbeing

At JSS Private School (JSSPS) we promote, develop, equip and prepare healthy learners for life. We are committed to making it our mission to promote resilience, positive wellbeing and mental health for all our pupils and staff. We understand wellbeing to be a state of being comfortable, healthy and happy. We aim to drive this message forward, and to ensure that mental health and well-being is "**everyone's business**" across the whole school community. We strive to create an environment that has a whole school approach, in providing excellent mental health support, understanding and intervention. We put Wellbeing at the heart of our school to ensure successful learning, and commit to our policies reflecting this practice.

## JSSPS Vision Statement on Inclusion

At JSSPS, we adopted a legislative frame work for inclusive education based on UAE Federal Law No.(29), 2006 & Law No.(2) 2014. The implementation and impact of the standards included within Dubai Inclusive Education Policy Framework (2017) are monitored and regulated by the Knowledge and Human Development Authority (KHDA).

We understand that a diversity and inclusion plan will be effective only when founded on a ***true belief in and understanding of the value of diversity and inclusion.*** Therefore, we aspire to create a school culture that reflects appreciation for diversity and inclusion at all levels. We know that our mission of driving personal and economic growth through learning and our vision of becoming the best community will only be achieved by hiring and retaining the best people possible while creating a school community that is reflective of the diverse audiences we serve.

JSSPS recognizes that the vibrancy of our community is enhanced by **diversity**, which we define as the range of human differences. We believe a culture of **inclusion** puts diversity into action by creating an environment of involvement, respect and engagement – where a multiplicity of beliefs, interests, experiences, and viewpoints are harnessed to accomplish our goals.

We work to achieve diversity and inclusion by:

- Delivering services in a culturally sensitive manner.
- Fostering an environment in which students and staff embrace and promote inclusion and understanding of the value of diversity as demonstrated through interactions with one another.
- Integrating diversity into strategies, decisions, and teaching-learning processes.
- Aligning diversity and inclusion efforts with strategic imperatives.
- Increasing effectiveness and accountability of efforts by developing measureable goals.

# INDEX


1. Introduction
2. Aims & Objectives
3. Roles & Responsibilities
   - 3.1. Principal
   - 3.2. IT Head
   - 3.3. E-safety Coordinator
   - 3.4. IT Coordinator
4. Software Usage
   - 4.1. Software Use
   - 4.2. Authorized Software
   - 4.3. Software Purchases
   - 4.4. Computer virus protection
   - 4.5. Retirement or Transfer of Licenses
   - 4.6. Computer Reassignment
   - 4.7. Microsoft Office 365
5. Hardware Devices
   - 5.1. Laptop
   - 5.2. Mobile Writing Pads
6. ICT Guidelines
   - 6.1. Student Guideline
   - 6.2. Teacher ICT Policy
   - 6.3. Internet
7. Cyber Safety
   - 7.1. Preventing Cyberbullying
   - 7.2. Guidance for Students for prevention and responding of
   - 7.3. Cyberbullying
   - 7.4. Guidance for Parents prevention and responding of Cyberbullying
8. Prohibited Content
9. Summary
10. Review of Policy
11. Annexure

## 1. 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, especially during the implementation of Distance and/or Blended Learningmodel(s).

Cyber Safety refers to staying safe online, and as internet-accessible devices are given to students, school is able to protect them from harmful content and services through remote learning platform Microsoft Teams.

Bullying is never acceptable and the school fully recognizes its duty to protect all of its members and to provide a safe, healthy environment for everyone.

## 2. AIMS AND OBJECTIVE

- To enable students to become autonomous, independent users of ICT, gaining confidence and enjoyment from their ICT activities.
- Use ICT as a tool to support teaching, learning and management across the curriculum.
- To ensure ICT is used, when appropriate, to improve access to learning for students with a diverse range of individual needs, including those with special needs.
- Children's ICT experiences are monitored and evaluated.
- Resources are used to their full extent.
- Staff skills and knowledge are kept up to date.

## 3. RESPONSIBILITIES

### a. Principal

The Principal will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

### b. IT Head

- Establish and review schemes of work for distance/blended learning model (in liaison with the MLT & SLT and Admin).
- Liaises with the KHDA / relevant body.
- Deploy support staff effectively where relevant.
- Maintain legible, accurate, comprehensive, records of formative and summative assessment results.
- Auditing the implementation, routine operation and maintenance of all IT related equipment and services in the school.
- Planning, procurement and deployment of upgrades in IT infrastructure to maintain a competitive, up-to-date and secure environment.

- Support and training of individuals and small groups of staff with their creation and use of multi-media content for teaching, research and conducting induction workshops.
- Keep up-to-date with latest education tools & ICT developments outside the school and bring them to the attention of colleagues.

### c. E-Safety Coordinator

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets regularly with IT coordinators to discuss current issues, review incident logs and filtering / change control logs.
- Reports regularly to Senior Leadership Team.

### d. IT Coordinator

- Running regular checks on network and data security
- Identifying and acting on opportunities to improve and update software and systems
- Institute protocols for the use of IT across departments.
- Provide advice on the most suitable IT choices
- Provide technical support for systems and networks
- Install and configure software and hardware (printers, network cards etc.)
- Monitor system and network performance
- Perform troubleshooting, repairs and data restoration
- Performance maintenance activities (e.g. backups)
- Maintain licenses and upgrade schedules

## 4. SOFTWARE USAGE

### 4.1 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 softwareor 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.

## 4.2 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.

## 4.3 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.

## 4.4 Computer virus protection

We have virus protection software on all computers. Students generally store their work on the hard drive, but some class disks are also used. Students are not allowed to take these class disks home, to reduce the risk of virus infection. However, some students 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.

## 4.5 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.

### 4.6 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.

### 4.7 Microsoft Office 365

- 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.
- Students and educators can sign up for Office 365 Education, including Word, Excel, PowerPoint, OneNote, and now Microsoft Teams, plus additional classroom tools. Use your valid school email address provided by the School IT Department to get the access.

## 5. HARDWARE DEVICES

### 5.1 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.
- Students to use their own devices with minimum required specification of windows 8 to have an access to effective Distance Learning through **Microsoft Teams.**

### 5.2 Mobile, Tablets&Writing Pads

School owned devices like telephones, tablet and writing pads 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 or School IT team.
- Specifically, the user is responsible for reporting lost or stolen device immediately to the IT Department.
- 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.
- 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 coordinator.

## 6. ICT GUIDELINES

### 6.1 Student Guidelines

- Students will access the Internet by following the net etiquettes and the internet guidelines provided by the school during their learning activity.
- Students to protect work by keeping their personal passwords private.
- 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

somessages 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, Digital cameras, Scanners, Printers and Interactive whiteboards shall result in the cancellation of privileges.
- Students are encouraged to access information that will enhance the learning programs usingMicrosoft Office 365. 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.

## 6.2 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 Team 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.

## 6.3. Internet

- Students are encouraged to use Social networking sites like Facebook.com/Instagram in a respectful manner.
- Use of the Internet is for study or for school authorized/supervised activities only.
- Use of ICT resources like Teams 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 online platform during Distance Learning.
- "Chat" privileges are enabled in Microsoft Teams to encourage effective communication among students, Teachers and peers.
- Respect the work and ownership rights of people outside the school as well as other students or staff. This includes abiding by copyright laws.
- All activities on Office 365are monitoredregularly.
- Students need to be aware e-mails sent and received, chat messages and groups created with/without teachers as a 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.

## 7. Cyber Safety

### 7.1. Preventing Cyberbullying

There is no single solution to the problem of cyberbullying but the school will do the following as a minimum to impose a comprehensive and effective prevention strategy:

- Ensure that all incidents of cyberbullying both inside and outside school are dealt with immediately and will be managed and/or escalated in line with the procedures set out in the school's Anti-bullying Policy, Behavioral Policy and Safeguarding and Child Protection Policy.
- Ensure that all policies relating to safeguarding, including cyberbullying are reviewed and updated regularly
- Ensure that all staff know that they need to report any issues concerning cyberbullying to the person-in-charge (Head of Pastoral Care)
- provide training (using Channel online awareness training module) so that staff feel confident to identify children at risk of being drawn into cyber bullying and to know how to make a referral when a child is at risk.
- Ensure that parents/guardians are informed and attention is drawn to the cyberbullying policy so that they are fully aware of the school's responsibility relating to safeguarding students and their welfare. The Cyberbullying Policy is available at all times on the school website.
- Ensure that at the beginning of each term, cyberbullying is revisited as part of the Staying Safe Programme and that pupils know how to report a concern to Class Teacher, Supervisor, Principal or Student Support Helpline (all contact details are available on school website www.jssspsdubai.com)
- Ensure that all staff are aware of their responsibilities by providing clear guidance for staff on the use of technology within school and beyond.
- Include lessons on online safety in computing lessons as part of their curriculum which builds resilience in pupils to protect themselves and others online.

### 7.2 Guidance for Students for prevention and responding of Cyberbullying

- If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, or school representative.

- Do not answer abusive messages but save them and report them
- Do not delete anything until it has been shown to your parents or a member of staff at school (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyber-bullying)
- Do not give out personal details or contact information without the permission of a parent/guardian (personal data)
- Be careful who you allow to become a friend online and think about what information you want them to see. Protect your password. Do not share it with anyone else and change it regularly
- Always log off from the computer when you have finished or if you leave the computer for any reason.
- Always put the privacy filters on to the sites you use. If you are not sure how to do this, ask a teacher/parent or seek a technical support
- Never reply to abusive e-mails
- Never reply to someone you do not know
- Always stay in public areas in chat rooms
- The school will deal with cyberbullying in the same way as other bullying. Do not think that because it is online it is different to other forms of bullying.
- The school will deal with inappropriate use of technology in the same way as other types of inappropriate behaviour and sanctions will be given in line with the school's Behavioural Policy.

### 7.3 Guidance for Parents prevention and responding of Cyberbullying

- It is vital that parents and the school work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying.
- Parents must play their role and take responsibility for monitoring their child's online activity.
- Parents can help by making sure their child understands the school cyber safety policy and, above all, how seriously the school takes incidents of cyber-bullying.
- Parents and school community should also explain to their children legal issues relating to cyber-bullying.
- If parents believe their child is the victim of cyber-bullying, contact the school as soon as possible and they should save the offending material (if need be by saving the offensive text on their computer or on their child's mobile phone) and make sure they have all relevant information before deleting anything.
- The school will ensure parents are informed of the cyber-bullying policy and the procedures in place in the Anti-Bullying Policy to deal with all forms of bullying including cyber-bullying.

## 8. PROHIBITED CONDUCT

The following provisions describe conduct prohibited under this policy:

- 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.

**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 denial of access to e- Learning Platform, 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 _____

Reviewed and Approved by

Mr. Govindarao Naik
Chief Executive Officer

Mrs. Chitra Sharma
Principal

Date:

## 9. SUMMARY

The ICT policy thus produces high quality documentation across the school and improve administrative practices by developing confidence and skills in ICT for staff and pupils which allows parents to access information more easily

Reviewed and Approved by Sd/-

Mr. Govindarao Naik
Chief Executive Officer

Mrs. Chitra Sharma
Principal

Date: 22/09/2023

## 10.REVIEW OF POLICY

The ICT & cyber safety policy will be reviewed by SLT on an annual basis.

| **Policy Details** | |
|---|---|
| Version date | May 2021 |
| Last review | September 2023 |
| Next review | September 2024 |
| Responsible SLT | Ms. Rajeswari V. |

## 11. ANNEXURE 1

# ACCEPTABLE USE OF TECHNOLOGY

JSSPS ACCEPTABLE USE OF TECHNOLOGY

*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 andapproved 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.

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 during Remote Learning.

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 repeatedly uses a technology in a manner that does not follow these guidelines (determined by the teacher or administrator), the student will be warned and brought to the further notice of parents and School 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 strict 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 during Remote Learning.Nor can any images or video recorded during online Learning sessions 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.

**Annexure**

CBSE Cyber Safety Handbook