INDIA INTERNATIONAL SCHOOL

A Heritage of Vision • A Legacy of Innovation

Hand Book on Use of ICT Facilities

2021-22

INDIA INTERNATIONAL SCHOOL

Shipra Path, Opp. V.T. Road, Mansarovar, Jaipur 302 020,

Ph: +91-141- 2786401-3, Fax: +91-141-2786404,

Email: iisib2012@yahoo.com, iis@icfia.org, Web: www.iisjaipur.org

Cambridge Assessment International Education

Cambridge International School

Vision

"A Heritage of Vision, A Legacy of Innovation."

Mission Statement

"The institution aims at uncompromising commitment towards holistic development and groom globally ethical citizens."

Philosophy

"IIS caters to the global need of today's youth, aims to engage learners in an active and creative learning journey, build knowledge and skills, promote and sustain high academic principles while retaining the strong value systems and ethics of the motherland and become caring members of global community."

Pedagogy

"We aim to nurture Caring, Creative, Independent Thinkers who are not only Disciplined but Open Minded as well."

Information Communication Technology – definition

Information technology facilities and resources are an integral part of the teaching, learning, research and administrative pursuit of IIS. The school recognizes the responsibility to ensure the appropriate use of its ICT facilities and that it must be protected from damage or liability resulting from the unlawful or inappropriate use of its ICT facilities.

It seeks to provide excellent facilities for academic and general staff, and to protect both the facilities and its users, and to ensure a productive and safe computing environment without imposing unnecessary restrictions that would detract from the school's culture of transparency.

The security of these facilities requires the support of all students and staff; therefore it is the responsibility of every student and staff member to understand this policy and to conduct their activities in accordance with it.

Aims of ICT:

1. To help students to become competent and confident users who can use the basic knowledge and skills acquired to assist them in their daily lives
2. To assist students to grow personally by facilitating different methods of learning.
3. To provide access to the ICT skills required for individuals to understand, analyse and utilise ICT as a wealth of tools that facilitate teaching and learning
4. To encourage an inquisitive approach in each individual
5. To help students become well-cultured citizens of the modern world

The Role of Technology:

Technology use is integral to IB constructivist approaches to teaching and learning and actively supports the curriculum. It is closely related to the basic tenets of an IB education (IBO 2013a: 2) Technology as part of an IB education aims to be:

Evident but seamless in the written, taught, and assessed curriculum Accessible to all learners, to be used to facilitate classroom environments that are inclusive and diverse by design, and useful in enhancing curriculum design and lesson planning.

Adaptive to many contexts: cultural, physical and educational Supportive of intercultural understanding, global engagement and multilingualism, specific hallmarks of an IB education.

Useful in collecting, creating, designing and analyzing significant content. The technology equivalents of the IB ideals emphasize the stance that technology use in the IB context supports the existing curriculum, and does not dominate it.

Technology use is compatible with the IB curriculum and can produce desirable outcomes when integrated with the concepts outlined in the individual programmes. Technology literacy is an aim of the IB programmes, and is one of the multi-illiteracies that are integrated in to a IB Education.

ICT Policy for CBSE and International Wing students:

Teaching using ICT at IIS is always promoted as it is emerging technology. To support this:

Smart boards are installed in class rooms (at least one on each floor) for which contract has been signed with Educomp and Extra Marks. Technical help is always available in case teacher needs. Annually training session is arranged for teachers. A team is appointed to handle the technical issues w.r.t smart board.

Students are also encouraged to use ICT lawfully. Briefing session is conducted for students on regular basis.

1. Students are not allowed to use internet/ wi-fi without permission
2. Eatables are not allowed while using ICT equipment.
3. In case of theft /destruction of the computers or peripherals, double the cost of the hardware will be charged from student / user
4. Hostlers must take prior permission from the hostel warden or concerned subject teacher in writing.

Workshop on Cyber Threat and Use of technology is conducted for teachers & students by IT department, which covers the following key points:

a. Phishing
b. Vishing
c. Smishing
d. ATM skimmers
e. Malware
f. Wi-fi Security

g. Netiquettes

h. Social networking & privacy setting

i. Cyber Law

j. Eavesdropping & snooping

k. Ransomware

l. Cyber Bullying

m. Online learning

As a regular annual feature, school shares few tips with parents in form of circular to bring awareness w.r.t Cyber Security. Also website will be updated with all handbooks on Cyber Security(for students, Teachers, parents & school) which is released by CBSE.

Policy on usage for International wing students (IBDP & IGCSE students)

Purpose

The purpose of this policy is to define acceptable use of computing facilities at IIS allowing students and staff to work confidently in the information technology infrastructure whilst safeguarding the integrity of the computer systems, networks, software and data. Inappropriate use exposes the school to risks including attacks from malicious software, disruption and compromise of network systems, devices and services, and legal issues thereafter followed by.

Scope

This policy applies to the use of all computing and network systems that includes LANs, wireless, modems, IB Resource Centre and computer labs and other areas in the campus rooms. This policy also applies to the use of ICT facilities by staff, students and visitors, including privately owned equipments.

Breach

The students will agree to strictly abide by this policy each time they access any of the facilities for the duration of their use of the facilities. Any breach of this policy may result in termination of accounts and/or disciplinary action up to and including suspension from school.

Agreement to the Policy

The students will be asked to sign a copy of the Use of ICT Facilities Agreement Form to acknowledge their acceptance of the terms and conditions of this policy before access is granted.

Few important terms (Definitions)

Computing and Network systems: Includes LANS, wireless and modems and telephone/ mobile phone on the campus.

Facilities: All computing facilities and services, provided in laboratories, resource centre and other areas on campus and services provided through remote access.

Spoofing: The act of constructing electronic communications to appear as though they came from another party.

Snooping: The act of monitoring the usage of any computer facility or the traffic generated by another user.

Spam: Unsolicited electronic communications. Examples of spam include, but are not limited to:

Unauthorized mass emailing and messaging of any unauthorized nature among each other.

Forwarding chain letters or electronic "petitions", or asking recipients to forward messages

Soliciting financial support or otherwise for charity, or special causes not related to any CAS activity in the school.
Sending unverified public service announcements (such as virus alerts, unsafe products, lost and found, etc.)

Hacking: Where e-mail messages, otherwise viewed as spam, are sent to as is appropriate to a school's electronic mailing list, may not necessarily be classed as spam.

The act of gaining unauthorized access to school's computers, networks, information systems and / or other user accounts, via a local or remote communication network.

Students are expected to be good Online citizens

- Be careful while posting any content, posters, material, pictures online.
- Use social networking sites carefully and safely.
- In case of any fraud or cyber threat, report to your elders immediately.

- Parents to set standards for what your child can and cannot do online. Regularly monitor your child while he/ she is online
- Privacy settings on social media platforms enable you to select who can access your posts online. Try to restrict access of your profile to your friends only. Remember what you post online remains there almost forever.
- Try to use known Wi-Fi links, which are password protected. Don't connect to an unknown or unrecognized Wi-Fi. Treat all public Wi-Fi links with suspicion.
- Avoid logging into websites where there's a chance that your identity, passwords or personal information may be compromised.
- Install anti-virus software and ensure that it is updated regularly.
- Do not always trust your new-found online. Remember, the predator waits patiently, so be careful.

Acceptable use of IT Facilities

ICT facilities are provided to the students and staff as an information disseminating tool; however, using it for reasonable, incidental personal purposes is acceptable.
Personal use must not, however, detrimentally affect user productivity, disrupt the system and/or stake the reputation of the school.

The students and staff should take full responsibility for activities conducted using their computer and network accounts, and must not allow anyone else to use any of these accounts, and agree not to use any other person's accounts.

All IT facilities provided by the school to students and staff members remain the property of the school at all times.

The school makes no express or implied warranties or conditions with regard to the facilities or internet and assumes no responsibility for any consequence of service interruptions or changes or the receipt or delivery of any electronic communication.

The school reserves the right to immediately, and without notice, withdraw/suspend access to the facilities in case of violation.

The school reserves the right to monitor or review information stored on the facilities as well as Internet and email as necessary. Material communicated and received through the facilities is the property of IIS and may be checked by Systems Administrator and/or deleted. It also reserves the right to prevent communications to and from external persons in its sole discretion. The users in any capacity should hold no expectation of privacy while using the school owned equipment and facilities.

Students and staff must not bring food or drink into labs, or consume food or drink around or near any workstations in the computer labs or resource centre.

The school does not and cannot in any way supervise, edit or control the content and form of any information or data accessed through the facilities and that the school shall not be held responsible in any way for any content or information accessed via the facilities.

Software

Users may not download and install any malicious or illegal software without seeking written permission from the Systems Administrator.

Prohibited use of IT facilities

1. Any software owned or licensed by the school for the IB / IGCSE/CBSE curriculum is for use by the school; and outside the terms of the licensing agreements, it is illegal to copy onto CD, DVD, USB, or any other media and distribute any such software.

2. Students and staff must be aware that unauthorized duplication and distribution of software may expose an individual to penalties.

3. Eating & drinking nearby any ICT hardware is not allowed.

4. Students and staff must not use any of the facilities for an unlawful purpose, including, but not limited to the following:

   a. Infringing copyright or any other intellectual property right in any way, and in particular by copying, accessing or downloading, or assisting with the use, acquisition, distribution, broadcasting or public screening of, any software or other copyright protected material (such as MP3s or DVDs) without a license.

   b. Using shared drives of computers connected to the campus networks to provide access to, or to distribute, infringing material, whether the drive is freely accessible or password protected, and whether the computer is owned by the school, students or staff.

   c. Sending, receiving, storing, displaying, printing, uploading, downloading or otherwise disseminating material that is fraudulent, illegal, embarrassing, sexually explicit, obscene, intimidating, or generally inappropriate except when required for approved teaching, learning or research purposes. While the school encourages critical analysis and review of cultural and social

norms, it does not condone unlawful, insulting or demeaning behavior. Hence, the users are expected to take account of the sensitivities of other users.

5. Students and staff members must not use facilities to perform any action that would bring the school into disrepute. This includes, but is not limited to, dispersing internal or confidential data without proper authorization.

Instructions on Username and password

Users(Staff members / Students/Parents) will be given account on various platform for e.g. ERP, Microsoft Teams App/ My IB/ Cambridge Teacher Support/ School Exam Portal/ etc. Users will be expected to keep the login credentials confidential and must not share with anyone.

Users are responsible for all activity initiated from their accounts, unless it is established that the activity was done by another person who gained access to the user's account through no fault of the user

Users must select passwords that cannot be easily guessed and they must not divulge passwords to others, including other students and staff. Resetting of password for any platform may take 2 – 3 working days.

Users must not attempt to determine another user's password. If the security of a password is compromised, the password must be changed immediately.

Users are not permitted to authorize others to login using their account except where ICT has requested such access for diagnosis and/or software installation.

The passwords should be changed at regular intervals.

Security

Users are prohibited from knowingly accessing or attempt to access any of the facilities for which they do not have authority.

Users must take all reasonable steps to maintain facility security at all times and to immediately report any security breaches to the Systems Administrator.

Users are obliged to run the school's chosen anti-virus software on a regular basis to protect devices from any threat.

Users are responsible for activities conducted using their accounts. Any information stored on a computer's hardware is the responsibility of the user and they must take reasonable precautions against the discovery of their passwords by other persons and comply with any schools' password policy that is in force.

Users should not permit or aid unauthorized persons to use the schools computing facilities.

Privately owned equipment

Users may connect privately owned electronic equipment to the school's networks on campus for the purpose of undertaking legitimate activities relating to their roles at IIS subject to the following conditions:

Any such connection, disconnection and use of privately owned electronic equipment is to be approved by ICT.

Connection is only permitted if there is no potential risk to IIS facilities or possible interference with other users. Private electronic equipment must have an effective antivirus solution and all installed software must be licensed.

Monitoring the use of ICT facilities

The ICT management reserves the right to monitor any and all aspects of its ICT facilities to determine if a user is acting unlawfully or violating this policy.

Monitoring the usage of any computer facility or the traffic generated by another user is illegal.

The Systems Administrator is authorized to access the student and staff accounts, email and storage areas wherever/whenever necessary to ensure the security, integrity and efficient operation of facilities.

ICT management will keep a record of all requested accesses, and notify the account owner of the access.

Users may not attempt to use any tools, technologies or systems to conceal any behaviour on their part that contravenes this policy. ICT management has the right to counter those tools, technologies or systems, in order to assess breaches of this policy and to protect the school's property.

Where there are reasonable grounds for suspicion of serious misuse, at the discretion.

And, upon written approval of the DPC, the systems administrator may access any hardware without notice to the user or relevant association.

Tampering

1. Users must not interfere or attempt to interfere with the operation of any computing facilities, including hardware, software, files, and access by authorized users including by propagation of computer worms and viruses.

2. Only the systems administrator or ICT staff, or those with written authorization, are permitted to perform any amendment or maintenance on facilities on the campus. Users may not operate any server or device that may compromise the operation of the school's network (including DHCP, DNS, WINS, email, domain controller or LDAP server), on their computer, from any port on the network including the resource centre without the express approval of the Systems Administrator. Where such servers are found to be running, at the discretion of the Systems Administrator, the network port for that device will be disabled, disconnecting that device from the network, and any associated user accounts will be disabled, pending removal of the offending device.

After Effect → Covid-19

Keeping in mind teaching – learning may be blended / online for the session:

Blended Learning model includes both an Asynchronous Learning Environment as well as Synchronous, real-time engagements. An Asynchronous Learning Environment is a learning environment that does not require participants, teachers, and students to be online at the same time. (For classes 1 to 5)

Synchronous, real-time engagements are opportunities for students to participate in engagements with their teachers and classmates at an established time to allow for interactions in real time. (For classes 1 to 12)

The following Plan is designed to address the following scenario:

- Asynchronous learning to ensure the opportunity to learn for all students in all time zones;
- Synchronous engagements to support learning and socio-emotional well-being of students through real-time engagements;

IMPORTANT POINTS FOR STUDENTS:

- Your device should be compatible for Microsoft Teams App
- Ensure you have a good bandwidth internet connection.

- Be organized before the class. Join the meeting 5 mins before the scheduled time
- Find a suitable quiet place (free from distractions) along with your books, notebooks & stationery.
- Must promptly read / respond to the notifications sent on Teams by your class teacher / subject teacher

Join the class with your name profile

- Do not share the meeting id and password with anyone.
- Treat your teacher and class mates with respect during online class
- If a child is absent, parents are requested not to attend the class in place of their child.
- **"Balance screen time with green time"** : Meaningful screen time is recommended.
- Students should not chat unnecessarily in the chat box. Only share your doubts through the chat box. Be careful what you write or upload online
- Keep your microphone on Mute mode. You may unmute only if it is required (if asked by your teacher)

Staff member must:

- Be well IT equipped for online teaching, online assessments and online evaluation
- procure personal laptop, connector (if required) for connecting internet to laptop and hotspot(if required)
- run anti-virus software and keep such software up to date by regularly installing the latest signature files;
- run personal firewall software and will ensure that such software is configured appropriately and kept up to date; and

- will download and install the latest security patches for your operating system and web browser regularly and pay heed to security notices and advice issued by your operating system and web browser vendors

Initially Teaching – Learning process took place via Zoom & Webex but School purchased Microsoft Teams a secured and customized LMS. Individual logins were created for each teacher and student. All important study material, notes, worksheets, assignments, etc are shared via Teams app.

Online assessments are conducted through Teams App. Before each examination IT department briefs students / teachers on technical points. A briefing session on the following is also done for students:

i. Camera to be switched on full time
ii. Time management
iii. Academic honesty
iv. Virtual invigilation

School opted Google Meet and Google Classroom also. Submission of drafts of NEC/IAs is done through Google Classroom, further Teacher-student interaction for Orals, feedback on IAs/ NEC, doubt clearing, etc is been done via Google Meet.

During completion of NEC, if required student conducts online interview / interaction with client via Google Meet.

A Session – "Awareness on Cyber Security" will be conducted with parents on PTM"

IT department will provide all IT support to all stakeholders as and when required.

IT based activities planned keeping latest IT trends, like which enhance students' IT skills and LP attributes as well:

1. Online coding
2. App Development
3. Creating animation-based stories
4. And many more

Implementation and review

All HODs, IT Head, Systems Administrator, Heads of School, IBDP Coordinator and other equivalent will be responsible for the implementation of this policy in their respective areas of responsibility.

The ICT department of the school is responsible for regularly reviewing this policy in coordination with the DPC and other HODs as the need be.

The ICT department has authority to recommend amendments to the policy and any associated procedures.

Communication

The ICT department is responsible for ensuring that all students and staff have access to this policy through the school's website.

This policy will be included in the information package provided to all new enrolling oncampus students during admission.

Disclaimer

This policy is intended to provide a framework to cover the broad areas of activity and establish principles required to govern operations within a secured and protected environment.

It is acknowledged that it is not possible to anticipate every situation that will arise, and as a consequence students and staff will be required to make informed decisions within the guidance and general directions provided by the policy.

Indemnification

The users agree to indemnify the school for any loss arising out of a breach of the rules contained in this policy and the associated agreement, including but not limited to a breach of any third party's intellectual property rights.

Committee Members:

- Dr. Ashok Gupta, Director & Head of School
- Mr. M.L.Agarwal, Academic Advisor
- Ms. Mala Agnihotri, Principal and IBDP & CIE Coordinator
- Ms. Nidhi Mishra, Assistant Prinicipal
- Ms. Mukta Khandelwal, DPC & International Wing Head
- Ms Jyotsna Dhamechani, Examination Head & IGCSE Coordinator
- Ms. Sarabjeet Kaur, CPP & CLSP Coordinator
- Ms. Prabhjeet khanna, HOD-IT,
- Ms Shilpi goyal – IT Faculty
- Mr. Vishnu Modi, IT Coach & System Administrator

Bibliography & Referencing:

- The role of technology in the IB programmes (pre-publication)
- https://ibo.org/copyright
- www.google.co.in (for images)

Updated in March, 2021