



بیلوا انڈیان سکول
BILVA INDIAN SCHOOL

Vision

Our vision is for all students to develop at Bilva Indian School as independent learners with self-belief and respect for others, with a lifelong love for learning and a strong foundation for future success

ICT policy

Our aims in using ICT in Learning and Teaching are to:

- Extend and enhance learning across all areas of the curriculum.
 - Contribute to raising standards in literacy, numeracy and other areas of learning.
 - Encourage pupils to select and use ICT appropriate to the task.
 - Develop skills in the use of ICT and the ability to apply these skills in a range of curricular contexts.
 - Give children access to a variety of sources of information.
 - Instil in children a sense of confidence, achievement and enjoyment.
 - Enable pupils to extend their learning beyond the school environment.
 - Ensure teaching staff are motivated and skilled in the use of ICT and aware of the contribution ICT can make to learning and teaching.
-
- Enable pupils to develop the skills of using ICT safely and responsibly in a safe learning environment.
 - Use of ICT will catalyse the cause and achieve the goals of inclusive education in schools.
 - Rigorous and continuous scanning of peripherals devices for anti viruses.
 - Firewalls in place to ensure safe viewership of online content.
 - Support of various software such as Photoshop, MSW LOGO, i Tell, Flash Player etc to enhance student learning

Our aims in using ICT in School Management are to:

- Create, use and adapt high quality digital teaching resources.
- Support communication with parents and the wider school community.
- Encourage sharing of resources and good practice through ICT.
- Increase professional efficiency through the use of ICT systems for planning, record keeping, reporting and communicating.
- Enable the use of pupil performance data to inform strategic planning.

STRATEGIES FOR USE OF ICT

- Since the focus of the Bilva Indian School Curriculum has been on 'Using' ICT skills, ICT is not being taught as a distinct subject to Primary Section, but is a tool to be used in a variety of meaningful contexts throughout the curriculum and Senior School pupils can seek career opportunities through extensive and effective use of ICT skills
- ICT is planned and delivered as an integral part of each curriculum area to support and enrich children's learning.
- All pupils are given equal access opportunities in using ICT resources.

PERMITTED USE OF INTERNET AND SCHOOL COMPUTER NETWORK

The computer network is the property of The Bilva Indian International School and is to be used in an efficient, ethical and legal manner for legitimate educational purposes, improving intellectual knowledge. Students are provided access to the computer network to assist them to carry out their subject related research work, and collaborative on the network. Abuse of the computer network or the Internet, may result in disciplinary action, including possible termination, and civil and/or criminal liability.

Computer network use

limitations: Prohibited Activities:

Without prior written permission from school, the school's computer network may not be Used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive codes (e.g. viruses, self-replicating programs, etc.), pornographic text or images, or any other unauthorized materials. Students may not use the school's internet connection for personal work, activities not of educational value, to download games over the internet for personal use. Additionally, students may not use the computer network to display, store or send (by e-mail or any other form of electronic communication such as bulletin boards, chatrooms, social networking sites, etc.) material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, destructive, intimidating, defamatory or otherwise inappropriate or unlawful. The students will not use the internet for violation of the privacy of any person, contact with questionable persons and for any destructive behavior. Furthermore, anyone receiving such materials should notify his/her Head of the School immediately.

The students are prohibited from doing or committing any act of Vandalism i.e. malicious Attempt to harm or destroy hardware, software, and data of another user, internet or any other network. This includes, but is not limited to creation, uploading of any virus.

Illegal

Copying:

The Students may not illegally copy material protected under copyright law or make that Material available to others for copying. Students are not supposed to download any software/ material for which a registration fee is charged without first obtaining the express written permission of the school.

Communication of Trade Secrets:

Students/Parents are prohibited from sending, transmitting, disseminating or otherwise Distributing proprietary information, data, trade secrets or other confidential information belonging to school. Unauthorized dissemination of such material may result in severe disciplinary action as well as substantial civil and criminal penalties under state and federal Economic Espionage laws.

DUTY NOT TO WASTE OR DAMAGE COMPUTER RESOURCES

Accessing the Internet:

To ensure security and avoid the spread of viruses, students accessing the internet through a

computer attached to school's network must do so through an approved Internet firewall or other security device. Bypassing school's computer network security by accessing the Internet directly by Wi-Fi or other means is strictly prohibited unless the computer you are using is not authorized to connect to the school's network. Students should access the internet only when it is required to carry out their research work.

Frivolous

Use:

Computer resources are limited & expensive. Network bandwidth and storage capacity Have finite limits, and all students connected to the network have a responsibility to conserve these resources. These acts include, but are not limited to, taking unnecessary printouts, sending mass mailings or chain letters, spending excessive amounts of time on the internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing unnecessary streaming of audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-educational uses of the internet.

Virus

Detection:

Files obtained from sources outside the school, including disks brought from home, files, downloaded from the internet or other online services, files attached to e-mail, and files provided by other staff, may contain dangerous computer viruses that may damage the school's computer network and the students should try to avoid use of such files, disks etc. on the school's network. Students should never download files from the Internet, accept e- mail attachments from outsiders, or use disks from non-school sources, without first scanning the material with the school-approved virus checking software. If you suspect that a virus has been introduced into the school's network, notify the school immediately.

NO EXPECTATION OF PRIVACY

Students are given computers and internet access to assist them in their study Work. Students should have no expectation of privacy in anything they create, store, and send or receive using the school's computer equipment. The computer network is the property of the school and may be used only for school purposes.

Monitoring of Computer and Internet

Usage:

The school has the right to monitor and log any and all aspects of its computer system Including, but not limited to, monitoring internet sites visited by staff, monitoring chat and newsgroups, monitoring file downloads, and all communication sent and received by students.

Blocking Sites with Inappropriate Content:

The school has the right to utilize software that makes it possible to identify and block Access to internet sites containing sexually explicit or other material deemed inappropriate in the school.

PROTOCOLS FOR USING ICT FACILITIES IN SCHOOL:

Use of Computer Systems in School

The school's ICT facilities are available in the ICT Lab, libraries and in every classroom.

The following procedures must be followed while using them:

- Users may access their accounts by logging on to the school domain with their username and password.
- Please use remote control for switching On/Off the projector in classroom / workstation.
- To avoid damage to the projector, do not switch it off directly from the main panel. Wait till the lamp is cooled and the red light stops blinking, before doing so.
- Students are not allowed to use the above ICT resources without the permission of a teacher. Students use the "Student" login to connect to school domain.

Use of Wireless Connection in School

- Access to the Wi-Fi connection is available for authorized staff.
- Your laptop will be allotted an IP address by registering its Mac address with the school.
- Bypassing the school's computer network security by accessing the Internet directly by Wi-Fi or other means is strictly prohibited.
- Select the school's wireless network option using your laptop Wireless Network Connection Manager.
- You may now launch your browser to access the Internet.
- Please note that the school reserves the right to monitor anyone's computer system and internet sites accessed by any guest, student or staff member.
- The school also reserves the right to block sites with content that is deemed inappropriate.

Responsible / Safe usage of ICT facilities

1. Access must be made via the user's authorized account and password, which must not be given to any other person.
2. The computers in the computer rooms must not be left logged in unattended. It is not permitted to lock the computers.
3. Users should not access other people's files unless permission has been given by the files owner of the files.
4. It is not permitted to install, use or distribute illegal copies (pirate copies) of licensed software.
5. It is not permitted to play games on the computers.
6. It is not permitted to change the operational mode of the computers.
7. Report any hardware or software related problem to ICT Department. Don't try to troubleshoot the- problems on your own.
8. No Eatables are allowed in the ICT facility Centers.

In case of any damages to the ICT infrastructure, those responsible are liable to compensate the school for the same.

6. ACCEPTABLE USE

The use of the Bilva Indian International School technology resources is a privilege, not a right. The Privilege of using the technology resources provided by the School is not transferable or extendible by students to people or groups outside the school.

6.1 Parent/Guardian Responsibilities

Talk to your children about values and the standards they should follow on the use of the internet just as you do on the use of all media information sources such as television, telephones, movies, and radio.

6.2 School Responsibilities are to:

- Provide internet access to its students.
- Provide internet blocking of inappropriate materials as able. (Parents should also set internet controls at home).
- Provide network data storage areas. These will be treated similar to school lockers. Bilva Indian School reserves the right to review, monitor, and restrict information stored on or transmitted and to investigate inappropriate use of resources.
- Provide staff guidance to aid students in doing research and help assure student compliance of the acceptable use policy.

6.3 Students Responsibilities are to:

- Use all devices in a responsible and ethical manner.
- Obey general school rules concerning behavior and communication that applies to computer use.

Use all technology resources in an appropriate manner so as to not damage any school equipment. Use of any information obtained via the Bilva Indian School designated Internet System is at your own risk. The Bilva Indian School specifically denies any responsibility for the accuracy or quality of information obtained through its services.

- Help Bilva Indian School protect our computer system/device by
- Contacting an administrator about any security problems they may encounter.
- If a student should receive email containing inappropriate or abusive language or if the Subject matter is questionable, he / she is asked to print a copy and turn it into the office.

6.4 Student Activities Strictly Prohibited:

- Illegal installation or transmission of copy righted materials.
- Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, or sexually explicit materials .
- Use of chat rooms, sites selling student work.
- Internet/Computer Games.
- Downloading unauthorized apps.
- Spamming- Sending mass or inappropriate emails.

- Gaining access too other student's accounts, files, and/or data.
- Use of the school's internet/e-mail accounts for financial or commercial gain or for any illegal activity.
- Students are not allowed to give out personal information, for any reason, over the internet.
- Participation in credit card fraud, electronic forgery or other forms of illegal behaviour.
- Vandalism (any malicious attempt to harm or destroy hardware, software or data, including, but not limited to, the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and /or damage software components) of school equipment will not be allowed.
- Transmission or accessing materials that are obscene, offensive, threatening or otherwise intended to harass or demean recipients.
- Bypassing the B.I S Web filter through a web proxy.

6.5 Legal Propriety

- Comply with trade mark and copyright laws and all license agreements. Ignorance of the law is not immunity. If you are unsure, ask a teacher or parent.
- Plagiarism is a violation of the P.I.S Code of Conduct. Give credit to all sources Used, whether quoted or summarized. This includes all forms of media on the Internet, such as graphics, movies, music, and text.
- Use or possession of hacking software is strictly prohibited will result in Disciplinary action by the School.