BAL BHARATI PUBLIC SCHOOL

An Institution of Child Education Society (Regd.), Delhi

IT POLICY FOR SCHOOL OWNED DEVICES

Bal Bharati Public School, strongly believes that the usage of Information Technology is beneficial in the education domain. It recognizes the need to proactively educate the young learners and other users at school about the potential risks and safety hazards associated with technology and the internet. This document articulates the guidance, expectations and obligations of all devices of Bal Bharati Public School.

TABLE OF CONTENT

FEEDBACK FORM

The IT Department at Bal Bharati Public School aims to: -

1. Enable all users to access IT capability at the appropriate level.
2. Be aware of and respond to individual needs.
3. Respond positively to all users.

Areas under Operation: -

1. Information Technology– Network and connectivity both Wired and Wireless, Internal and outside world, Internet service and management, Servers, Desktops, Laptops, Printers, Scanners, Biometric devices and other electronic equipment.
2. Electronic Surveillance– CCTV System.
3. School owned\vendor software.

IT Helpdesk: -

1. Helpdesk operating hours are 8:30 AM TO 4:30 PM Monday through Friday and on all working Saturday.
2. IT \ Vendor Engineers (IT Engineer stationed in school) are the first point of contact for all IT related issues for Bal Bharati Public School.
3. IT engineers will maintain a register to keep the record of all the issues\complaints coming to IT helpdesk and will get it signed by the users.

Internet Access: -

1. There are different categories of control policies for different users for accessing the internet depending upon the group they are covered into such as IT LABS ,Other labs, Teachers, Staff, Administrators, Management, Free Access etc. as decided by the management.
2. No heavy applications that create unwanted network traffic and block accessibility for others except authorised person (e.g. Chat applications) is allowed.
3. Any required application may be downloaded & installed, but download access will be granted to some users only. An IT engineer can download any application, within the guidelines of the policy.

4. Based on the internet usage policy: internet connectivity of users crossing the allowable limits will automatically be blocked by the server. Here limited internet usage means filtered websites & categories which will be defined in the firewall policy.
5. Any special request for a special task on the internet. heavy download, restricted site access etc. will only be considered when user provides an authorization from respective HOD/HM/Vice Principal/Principal
6. The following guidance and precautions may be taken to avoid the risks associated with the internet.
   a. The staff should not use social networking sites if the students are in vicinity. Often, products advertised on these sites have no connection with education and can distract the student.
   b. If an innocent search on the internet leads to an inappropriate site, the window should be closed or minimized immediately. The staff may want to offer a simple explanation to student as per the age group
   c. As all computers are connected to the internet, it is important that students are supervised when working on the computers.
   d. The students and staff should refrain from internet requests seeking personal information, receiving inappropriate content, viewing incitement sites and on-site gambling sites
   e. The students are not allowed to surf the social networking sites at school.
   f. Chat-rooms, Discussion forums, messaging may be used only for educational purposes.
   g. The users -both staff & students are advised not to by-pass the filtering/blocking software.

1. Hardware and Software Policy:

1.1 IT engineers are normally equipped with most of the common drivers/patches etc. of hardware of major brands. Still the models/companies running in huge numbers, It is practically impossible to have all the drivers/patches etc. handy all the time.

1.2 No user is authorized to change/tamper with any data not belonging to him/her or his/her.

1.3 Avoid storing your personal information in the official Laptop/desktop, instead purchase your own Hard disk to do so.

1.4 Always scan the external devices through “Seqrite” before doing any data transfer.

1.5 BBPS maintains an Anti-Piracy Policy. We support and adhere to international copyright laws. Users should never download or install any commercial software, shareware, or freeware onto network drives or disks, unless they have the permission from the IT department to do so. Users should never copy other people's work or intrude into other people's computers / disks / files etc.

1.6 No user is allowed to bring any kind of inappropriate software to the school. All educational software is provided by the School.

1.7 Users will respect the school standards & Policies as and when Management decides and necessitated by Information Technology.

1.8 Users are not allowed to exchange their device with others or take the device out of school campus, without permission.

1.9 To understand the policy for Procurement of any hardware device or software, please refer to the Annexure "Procurement & Disposal of devices".

2. Network & Security Policy:

2.1 School will assign a Network Administrator from the team of technical staff and that person will monitor the Network security & will take the assistance of the IT Manager for any issue or new requirement.

2.2 Schools are using the Local Area Network in the campus and all the devices are connected through wired or wireless Lan. W-Lan's are secured with the encryptions.

2.3 For the security of the devices – Seqrite Antivirus is installed on the devices to keep them secured and software firewall is installed to control & monitor the web filtering.

2.4 All the devices will be regularly updated with the latest version & patches of antivirus.

2.5 In future the hardware firewall will be installed to monitor the network security and filtered internet services with the different web filter & application filter settings.

2.6 Detailed security structure & policies will be explained in the Firewall Policy, which will be issued after the Firewall deployment.

3. General Responsibilities of IT Engineers & vendor company:

3.1 To provide routine support to teachers/staff.

3.2 Create user groups (for Seqrite & firewall) & manage them as per the requirement.

3.3 Installing all the important updates on a timely basis.

3.4 Deploying the security policies to different user profiles, as per the approvals.

3.5 Installation of any new App/software, with the approval of administrator or principal.

3.6 Uninstall / remove any app/software with the approval of Administrator/Principal.

3.7 Maintenance of all the devices – Weekly for IT labs & Monthly for other users.

4. General Responsibilities of LAB Assistant for IT Maintenance:

4.1 Regular monitoring of all the lab devices, during the class.

4.2 Maintaining the issue\receipt record in register.

4.3 Provide primary level assistance to students & teachers.

4.4 Will make the weekly hardware-software status report & get it signed by the Lab in charge teacher.

4.5 For any major issue/incident related to LABS/DEVICES he will report to the LAB incharge Teacher.

4.6 Should ensure proper upkeep of the equipment keeping it clean and dust free.

4.6.1 Clean it with soft dry cloth.

4.6.2 Don't use any spray/chemical or any other liquid.

5. TEACHER's & Staff:

5.1 Staff needs to sign Issue Voucher for the equipment provided to them for usage. And need to take proper care of the equipment and will be responsible for its upkeep.

5.2 Teachers\Staff will be responsible for charging the device, which are individually allotted to them. A lab assistant will be responsible for charging the Tablets through a charging cart. But teachers will monitor and ensure that devices are being charged on a daily basis and keep them ready for the students.

5.3 Keeping the devices safely in their cabinet.

5.4 Avoid storing your personal information in the devices.

5.5 In case of any damage/fault, it must be reported to the IT dept. immediately.

5.6 For any requirement – software / app / additional hardware device – teachers will send the request mail to the IT dept.

5.7 In case a staff wants certain changes/additions/up gradation/shifting etc. in any equipment, the same must be noted on the IT requisition form and submitted to IT dept. after necessary approval, if required.

5.8 All the departments and users must keep the backup of their important data on google drive and update it regularly.

5.9 No staff is authorised to format\reformat the device. The same will be done by the IT dept., if required.

6. Data Back-Up & Security

To keep a copy of data is the best practice of any organization. Taking some basic steps can prevent any type of mis happening e.g.- deletion by mistake, fire, theft, flood and vandalism.

6.1 For windows devices - Never save any data on Desktop , My Documents & C drive.

6.2 Use Google Drive to take the data backup & save a copy of your data.

6.3 Google Sync tool can be installed for automatic backup of your data.

6.4 Always check the sharing settings before sharing any data with anyone and give permission as per the requirement.

6.5 For working together in a team, upload the data in the shared drive folder, where different access rights can be given to the users.

7. Social Media Policy

7.1 **Introduction:** This policy provides guidance to school staff, students and parents on how to safely and productively use social media to maximize the range of benefits it offers whilst mitigating associated risks. In particular, it provides information on: responsibilities when communicating via school social media accounts inside or outside the School premises; expectations of school staff on individual personal and professional accounts; and expectations of students and parents in relation to social media. Kindly Refer the school Social Media Policy for detailed understanding.

7.2 Policy Objective:

7.2.1 To provide school staff, students and parents with information on School requirements and expectations regarding social media

7.2.2 To ensure a consistent approach across all school social media platforms

7.2.3 To ensure school staff, students and parents do not compromise their personal security or the security of School community

7.2.4 To set out the responsibilities of users of school social media accounts

7.2.5 To support users of school social media accounts to mitigate the risks associated with social media, protecting themselves as well as the School

7.2.6 To clarify the expectations of school staff using social media in an individual professional or personal capacity

7.2.7 To outline channels for escalation of issues or concerns.

8. G Suite

BBPS recognizes the enormous potential of Information Technology in education. And we are using the Google platform "G Suite" for online teaching & learning. G Suite is for the use of authorized users only. Every user is provided with private access credentials to access resources provided by the school. The credentials provided are to be used solely for the performance of assigned functions. Each user is responsible for all matters pertaining to the proper use of their access privileges.

All the users staff & students are provided with the official G suite account access for using the various G suite tools.

For Staff – firstname.lastname@domain\subdomain

For Student – studentid@domain\subdomain

Access of G SUITE TOOLS

S.no.	G Suite Apps	For Staff	For Student
1	Gmail	Yes	Yes
2	Drive	Yes	Yes
3	Calendar	Yes	Yes
4	Docs	Yes	Yes
5	Sheet	Yes	Yes
6	Slide	Yes	Yes
7	Forms	Yes	Yes
8	Meet	Yes	Yes (only join)
9	Classroom	Yes	Yes (only join)
10	Hangout Chat	Yes	No
11	Jamboard	Yes	No
12	Google Chrome Sync	Yes	No

13	Contact	Yes	Yes
14	Directory	Yes	No
15	Marketplace Apps	No	No

For MEET & CLASSROOM: Students have the limited access, they can’t create any classroom and similarly they can’t create a Meet event. They can only join the classroom or join the meet session. And further they do not have permission to record or stream the sessions.

8.1 To maintain the accounts security we are using Strong password policy : Create your password using min 8 & max 15 characters. It can be any combination of letters, numbers, and symbols. Users should not share their password with anyone.

8.2 In case a user forgets his\her password then they will send the request on support email I’d (support@subdomain) with a Cc to HOD\HM and class teacher in case of Student.

8.3 The email communication should be done only through the official email id only and should be polite & the BBPS values should be kept in perspective while writing emails.

8.4 The students and staff should refrain from sharing personal information known about colleagues with a third party without permission from person[s] concerned.

8.5 The Staff & Students will use the G Suite tools only for the official & educational purpose, they will not use any tool for any personal work or will not save any personal data.

8.6 The school reserves the right to monitor, inspect, copy and review the school accounts like (G suite) when there's a reasonable suspicion of violation.

8.7 In case the Staff\Student is leaving the school, then the G Suite account will be suspended.

8.8 Important Instructions for TEACHERS, while doing the Google Meet session

• Never allow the students to join the meeting, using personal email id.

• Share\Enable (Visible to students) the meeting code at the time of the class.

• Leave the meeting in the last.

• Reset the meeting code & then disable (Visible to students) it for students.

• Record the meeting – whenever required.

• If internet speed is slow, turn OFF your camera.

• To help students who are deaf or hard of hearing, turn on live captions in Meet.

• If you’re using a mobile device, install the Google Meet app on your device.

• Charge your device before the meeting. On devices like tablets and laptops, charging can reduce video quality.

8.9 Important Instructions for STUDENTS, while doing the Google Meet session:

- Please be ready 5 mins before the scheduled class.
- Keep your mobiles on silent if kept near your laptop / tablet.
- Take the session seriously and follow instructions given by the teacher.
- Mute your camera and mic and switch on only if you have a question by seeking permission from the teacher and Use a chat window to post your questions.
- Students should hang up once the session finishes.
- Parents should avoid interruption in between and allow the child to handle the session, in case of any query /issue post on the chat window.
- Use the incognito mode window for your online sessions. The easiest way to open an Incognito window is with the keyboard shortcut combination Ctrl-Shift-N (Windows) or Command-Shift-N (macOS).

9. Bal Bharati Connect

10. Exit of any Staff from BBPS

10.1 Any staff resigning / leaving BBPS has to mandatorily get clearance from the IT Department.

10.2 All the login id's given to the staff/student, and will be suspended before signing the clearance form.

10.3 Any staff resigning / leaving has to necessarily submit the equipment's issued to him/her at least 7 days before his/her last working day.

10.4 The equipment will be checked by the Helpdesk in terms of its fit working condition, any damage etc. Returned material inventory will be tallied with the one recorded in Helpdesk Records as issued to the user.

10.5 In the event of any defect/breakage etc. attributable to the user, the cost of the same will be ascertained and informed to the Accounts Department.

ACKNOWLEDGEMENT

I have read and been informed about the IT policy of Bal Bharati Public School. I have received a copy of the policy and agree to abide by the policy guidelines as a condition of my employment in the school. I also understand that if I have questions, at any time, regarding the policy, I will consult with my immediate supervisor or IT department.

I undertake to:

- Respect myself - Use BBPS computer network ~~and~~ with honesty and integrity. Keep standards of decency in accessing, viewing, or sending messages and pictures. Keep my password secure, support copyright laws;
- Respect other users - Respect other's work and files, their privacy, and their right to access the network, respect hardware, software, and peripherals that we all share;
- Respect the network management - Respect their need to oversee the running of the network. Have my devices configured in compliance to BBPS IT Policies. Get approval from the IT Department for any configuration change; add/ amend any software etc. on my Laptop/other IT devices.

I have read the policy carefully to ensure that I have understood the policy before signing this document.

Employee Signature:

Employee Name:

Employee Code:

Date:

Annexure 1

PREVENTIVE MAINTENANCE FORM

Date: ______________________________Time: ______________________

Username: ________________________ Dept.______________________________

Asset Details: ____________________Serial/Asset NO.: _____________________

Problems (Reported by user): ____

____

Problem found by Engineer (If any): ____

____

____

____

User Sign. ______________________________

Remarks: ____

Engineer Sign. ______________________________

Remarks: ____

<u>Annexure 2</u> **INCIDENT REPORT**

Name of Staff: ______________________Designation: _______________Department: _______________

Sr.	Product description	Incident Details (if any)	Problem reported (if any)
1			
2			

Signatures:__________________

Date: ______________________

HOD :_________________________

Signatures: __________________________

Problem diagnosed by IT Engineer and Action Taken

Manager IT Remark

Signatures:________________

Cost to be debited to:
(mandatory)

REQUESTER / SCHOOL
(strike off what is inapplicable)

Note: Further action and required time can be informed based on part's availability.

Annexure 3 REQUEST FOR SHIFTING OF DEVICE

IT Requisition Slip for Shifting / Modification

Name : ________________________ Designation: _________________________

Department: ______________________ Date : ___________________________

Task	New installation	Modification/shifting	Building/ Location	Floor/room	Remarks
Installation of computer					
Issuance of Laptop					
Any other					

Approved by: HOD/HM Principal: ___________________

Signatures:______________________ Signatures:_____________________

For IT use only

Feasibility checked on:______________________________

Engineer/Technician: _________________ Signature:______________________

Network Admin :____________________ Signature: ______________________

Comments: ____

Note: Further action and required time can be decided only based on feasibility.

Annexure 4

IT REQUISITION FORM

FOR CONSUMABLE ITEMS & OTHER DEVICES

S.no.	Item Name	Brand	Serial No.	Qty.	Remark

Remarks (if any):

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………

User Name …………………………..

Department ………………………….

Signature …………………………….

Date ……………………**Time** ……….

Return Details

Date & Time ………………..

Signature……………………….

Remark…………………………

For IT \ Admin Remarks

Device TAG: …………………………………..Issued/Installed By: ………………………….

Toner Type: : ………………………………….. Printer Reading: …………………………….

REMARKS:

………
……………………………………

Annexure 5

FORMAT FOR ISSUE & RETURNING IT ASSET TO IT DEPT.

DEVICE DETAILS: LAPTOP

MAKE: MODEL NO. Serial No.

S.No.	Parts	Status Yes/No	Remarks
1	Asset\Tag No. of device		
2	Charger		
3	Bag		
4	CD / Combo drive		
5	Battery		
6	LAN Port		
7	USB Port		
8	Modem Port		
9	Card Slot		
10	Card		
11	Touch Pad		
12	Central Mouse and Cap		
13	Keyboard		
14	Base Cover		
15	Front Cover		
16	LCD		
17	Front Lock (Left &Right)		
18	Speaker		
19	Screws		
20	RAM		
21	HDD		
22	Overall Physical Condition of device		

Name of User: ____________	IT Engineer.: ____________
Signatures: ______________	Signatures:__________________
Date:_________________	IT Admin:
Time: _________________	Signatures:__________________

Feedback Form

Dear Mr./Mrs./Ms.

In our endeavour to better our services, we would like to request you to please write about the experiences you had with the Information Technology Department.

We would also welcome your kind suggestions which will improve the functioning of our department.

Wishing you all the best in the life ahead.

With warm regards,

IT Manager

<u>User’s Feedback</u>

Good Practices

- Ensure the physical environment of your laptop/IT equipment to be SAFE, DUST-FREE.
- DRY AND SECURE. Take personal responsibility for the "CLEANLINESS" of your laptop, desktop, printer. Majority of problems in IT equipment are caused by dust.
- Ensure you have ANTI-VIRUS PROGRAM installed on your laptop/Desktop and the DAT is of a recent date.
- Don't mess with viruses – TAKE WARNINGS SERIOUSLY.
- Be wary of "STRANGE" e-mail messages– do not open ATTACHMENTS that sound inviting.
- Data Backup - Users are requested to keep the backup of their important data, on the allotted Google drive. (Linked with your official G suite account)
- Avoid sending bulk mail. Use BCC field if sending to more than 50 users.
- Regularly check your mails & calendar.
- Avoid sending heavy attachments.
- Avoid storing your personal stuff in the Laptop, instead purchase your own Hard disk to do so.
- NEVER share your login credentials (Username & Password) with anyone.

Do’s & Don’ts for IT LABS

DO’s	DON’T
Turn off the machine once you are done using it.	Do not eat or drink in the laboratory.
Report any broken plugs or exposed electrical wires to your teacher/lab assistant immediately.	Avoid stepping on electrical wires or any other computer cables.
Report fires or accidents to your teacher/lab technician immediately.	Do not open the system unit casing or monitor casing particularly when the power is turned on.
For any hardware, software, printer, paper or any other problems, please contact the lab assistant or IT teacher.	Do not remove anything from the computer laboratory without permission.
Operate the computers/laptops/devices with respect.	Do not insert metal objects such as clips, pins and needles into the computer casings. They may cause fire.
Use the computer labs for school work only.	Do not plug in external devices without scanning them for computer viruses.
Save your all-important data/files in google drive.	Always use strong passwords and do not share your passwords with anyone.
Shutdown the system after your class.	Students are strictly prohibited from modifying or deleting any important files and installing any software or settings in the computer.
Always visit the appropriate websites while using the internet.	Always be careful while sharing the online content with anyone. Specially pictures & videos

Do’s & Don’ts for Staff BYOD devices

DO’s	DON’T
Device should be of good configuration with the original windows.	Use of pirated windows license.
Microsoft office should be installed.	Use of pirated ms office and other software.
Antivirus should be installed.	
The LAN port should be working.	
The HDMI port should be working.	
Use the Sophos login credentials for accessing the internet in the school campus.	
Scan the pendrive / external drive before using it on the school devices.	