Dated: 01.06.2021

To,
The Principal
Bunt`s Sangha`s S.M.Shetty International School & Junior College
Powai, Mumbai-76

Sub: IT Policy

Respected Sir,

I am writing this letter for approval for International Section IT policy. Bunt`s Sangha`s S.M.Shetty International School & Junior College have completed IT Policy review and have approved International Section policy. This approval covers the period from June 1, 2021. I am writing for your positive reply & approval for the same.

Thanks & Regards

Mr. Ashok Shetty	Mrs. Mildred Lobo	Dr. Sandeep Singh
Asst. Manager-IT	Principal	General Manager A & A

Created by IT Dept

BUNTS SANGHA'S S M SHETTY EDUCATIONAL INSTITUTIONS, POWAI

INFORMATION TECHNOLOGY

POLICIES & PROCEDURES MANUAL

TABLE OF CONTENTS

Information Technology Use Policy

Section I – Introduction

The Bunts Sangha's S M Shetty Educational Institute IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the institution which must be followed by all staff. It also provides guidelines Bunts Sangha's S M Shetty Educational Institute IT Policy will use to administer these policies, with the correct procedure to follow.

Bunts Sangha's S M Shetty Educational Institute IT Policy will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

These policies and procedures apply to all employees.

A. Policy Users: For Use by Institutions Staff and Other Authorized Users of Information Technology Resources

B. Policy Statement: This policy deals with the provision of information technology resources by staff, students and other authorized users of S M Shetty Educational Institutions. These resources include, but are not limited to, SM Shetty Educational network, computer systems, Laptop, Printers, Scanners, Wifi, Business application and software, access to the Internet, electronic mail, telephony and related services.

The policy is based on the following principles, which must be adhered to by all those responsible for the implementation of this policy and to whom this policy applies:

- The information technology resources of the Institution are provided to support the teaching, research and administrative activities of the Institution;
- Authorized users are granted access to valuable resources, sensitive data and to external networks on the basis that their use of IT resources shall be responsible, ethical and lawful at all times;
- Data and information relating to persons and other confidential matters acquired for administrative and academic purposes shall be protected.
- All confidential information shall be protected from unauthorized and/or accidental disclosure; and Institutions IT resources must not under any circumstances be used to humiliate, intimidate, offend or vilify others on the basis of their race,gender,or any other attribute prescribed under anti-discrimination legislation.

C. Broad Overview :

1. **What is provided and why** - The information technology resources of the Institution are provided to support the teaching, research and administrative activities of the Institution. These resources include the SM Shetty Educational network, computer systems, Laptop, Printers, Scanners, Wi-Fi, Business application and software, access to the Internet, electronic mail, telephony and related services.
2. **Access** – This policy prescribes the conditions under which access to S M Shetty Educational IT resources is granted.

3. **Responsible Usage** – Staff and other specifically authorized users who are granted access to IT resources are required to utilize IT resources in a responsible, ethical and lawful manner.
4. **What is and is Not Acceptable Usage** – This policy, to which all staff and other authorized users should adhere, identifies what is acceptable usage including the personal use of IT resources.
5. **Breach of Policy** – This policy identifies the possible consequences should a breach of the policy occur.

Section II - Detailed Policy

A. Definitions :

Email & Messaging - Email means the Institution-provided electronic mail systems and computer accounts. Additional messaging facilities may include but are not limited to calendar and scheduling programs, chat sessions, IRC, newsgroups and electronic conferences.

Information Technology Resources (IT Resources) – covers all IT facilities including all computers, computing laboratories, lecture theatres and video conferencing rooms across the Institution together with use of all associated networks, internet access, email, hardware, dial-in access, data storage, data center, computer accounts, software (both proprietary and those developed by the Institution), telephony services and voicemail.

Personal information means information or an opinion (including information or an opinion forming part of a database) that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Publish – to make information available for access by others via any method or format, including, but not limited to, on a web page, email, or the use of peer-to-peer programs.

Authorized User – any person who has been authorized by the relevant Institution Officer/Supervisor to access any S M Shetty Educational Institutions, IT system or IT facility, including but not limited to:

- Staff of S M Shetty Educational Institutions
- Staff of any entity/company in which S M Shetty Educational Institutions has an interest
- Staff of any entity/company /organization with which their institution is pursuing a joint venture
- Students
- Consultants
- Visitors
- Honorary appointees
- Collaborative researchers
- Alumni

B. Issues Addressed :

1. Access Information Technology resources

Lawful Use: The use of IT Resources must be lawful at all times. Unlawful use will breach this Policy and will be dealt with as a discipline offence.

Unlawful use of IT Resources may also lead to criminal or civil legal action being taken against individual authorized users. This could result in serious consequences such as a fine, damages and/or costs being awarded against the individual or even imprisonment.

The Institution will not defend or support any authorized user who uses IT resources for an unlawful purpose.

1.1 Granting of Access

Access to IT Resources is authorized by the relevant S M Shetty Educational Institution Officer/Supervisor, and provided by institutional unit responsible for managing the IT Resource (e.g., the Library). Access is normally based on a need to access that IT Resource and an individual's current status with the Institution as recorded in the Institution's Human Resources database, Institution Alumni database or other database managed by or the Human Resources Division or Student and Community Services Division.

1.2 Access on contract expiry or authorised access period

Email and computer access will cease on expiration of employment or contract or end-date as recorded in the Human Resources database. For strictly professional or work-related reasons, staff and other authorised users may request that computer access be extended for a period up to 90 days. Approval must be given by Head of Department or equivalent.

1.3 Responsibilities

Regarding Use of S M Shetty Educational Institution Computer Accounts

Each authorized user is responsible for:

- The unique computer accounts which the Institution has authorized for the user's benefit. These accounts are not transferable;
- Selecting and keeping a secure password for each of these accounts, including not sharing passwords and logging off after using a computer; and
- Familiarizing themselves with legislative requirements which impact on the use of IT Resources and acting accordingly. The Institution takes no responsibility for users whose actions breach legislation.

1.4 Restrictions to Access

Users are expressly forbidden unauthorized access to accounts, data or files on Institutions IT Resources or any other IT resource. The Administrator of an IT Resource may restrict access to an individual user on the grounds that the user is in breach of this policy.

1.5 Third Party Access

Entities other than IT department may neither negotiate nor grant third parties access to the Institution's communications and network infrastructure. Applications for access should be made in writing to the Office of the Chief Administrator.

1.6 Domain Name Registration

All domain names for S M Shetty Educational Institutions projects/activities must be registered through the Office of the Chief Administrator. This requirement must be observed in all instances. Users should note it is the Institution who owns and controls the site not the person who registers the name.

1.7 Software License Restrictions

Use of proprietary software is subject to terms of licence agreements between S M Shetty Educational Institution and the software owner or licensor, and may be restricted in its use.

2. Personal Use of Information Technology Resources

2.1 Extent of Personal Use - A user who is authorized to use the IT Resources may also use the IT Resources for limited, incidental personal purposes. Personal use of the IT Resources is permitted provided such use is lawful, does not negatively impact upon the user's work performance, hinder the work of other users, or damage the reputation, image or operations of the Institution. Such use must not cause noticeable additional cost to the Institution.

2.2 Commercial Use

IT Resources must not be used for private commercial purposes except where the paid work is conducted in accordance with the Institution Practice or the work is for the purposes of a corporate entity in which S M Shetty Educational Institution holds an interest.

2.3 Reasonable Use Determination

Whether or not use was reasonable in the particular circumstances will be a matter to be determined by the user's Head of Department or Administrative Head.

2.4 Institution Liability

The Institution accepts no responsibility for:

- Loss or damage or consequential loss or damage, arising from personal use of the Institution's IT Resources.
- Loss of data or interference with personal files arising from the Institution's efforts to maintain the IT Resources.

3. Internet Access

3.1 Access to the Internet: To lay down the rules & regulation governing usage of internet connectivity for enhanced operational performance & adherence to legal, security & safety requirements. Institute is using primary ISP as well as secondary ISP.

3.2 Work Purposes: Authorized users are permitted to access the Internet for work related purposes

3.3 Objective: Objective for community access to the Internet are:

- To increase understanding of the potential for learning and communication that the Internet
- Offers.
- To encourage and support a commitment to life time learning
- To fulfil educational department requirement and developing skill sets.
- To utilize unlimited technical knowledgebase available on Internet for troubleshooting day to day
- peculiar technical problem

3.4 Personal Usage: Access is also permitted for personal purposes provided such use is lawful and reasonable in terms of time and cost to the Institution.

Examples of permitted personal use are:

- Online banking,
- Travel bookings
- Browsing

3.5 Inappropriate Use of the Internet: When accessing the Internet from institute, you must ensure that the service is only used in accordance with policy. The following are examples of improper use:

- Accessing, browsing, downloading, storing or forwarding material which is, or could be considered to be, obscene, offensive or of a sexual nature, whether in word, image or audio file.
- Accessing, browsing, downloading, storing or forwarding material that is sexist, racist or could Offend others because of its political nature.
- Running a private business via the Internet e.g. selling, advertising.
- Contributing to Internet newsgroups and chat rooms or similar for without being authorized to do so.
- Downloading anything that constitutes an infringement of copyright, including images, music files and video in any format.

3.6 Monitoring of Internet Access: Internet access servers have the ability to record all access in a log detailing the originator. You should be aware that all access to the Internet from the Intranet may be intercepted, monitored and analyzed in accordance with legislation relating to such monitoring. Content filtering is done. Sites blocked like sex, porn etc.

3.7 Internet Connection of PCs: institute PCs must not be directly connected to the Internet. All access to the Internet must be controlled via the institute Firewall.

3.8 Reasonable Use Determination: Whether or not use was reasonable in the particular circumstances will be a matter to be determined by the user's Head of Department or Administrative Head.

3.9 WIFI D Creation: WIFI ID of the newly joined staff (both teaching and non-teaching) shall be created (If require) within 03 days of receiving the Notification from reporting Manager. For WIFI ID creation requires employees of the SM Shetty shall be provided with a unique identity using his/her First Name and Last Name within 03 working days.

WIFI ID Creation form:

Confidential WIFI 13-Jul-22

Bunts Sangha's S M Shetty Educational Institutions
WIFI Access Creation Request Form

General Manager A & A/ Principal/Vice Principal/HOD must fill out the Wi-Fi request form with your approval. User will visit the IT department along with approved Wi-Fi request form and device for Wi-Fi activation.

Wi-Fi Request From					
1 Hour Pin	2 Hour Pin	4 Hour Pin	1 day Pin	Permanent(MAC address binding)	Time Bound

Sr. No	Employee/Student Name	Department	Designation	WIFI request	User Sign

Please fill clearly and accurately the required information below. All information requested must be entered for this form to be processed.

General Manager A & A/ Principal/Vice Principal/ HOD

First Name: _____

Last Name: _____

Title: _____

Department:_____

Access Authorization: I certify the above usernames are authorized to access Bunts Sangha's S M Shetty Educational Institutions Wi-Fi and grant permission.

_____

General Manager A & A/ Principal/Vice Principal/Coordinator/HOD Signature

IT Dept. use only

Wi-Fi User name: _____Created date: _____

Wi-Fi was created on: _____Creators name: _____

1

4. Email and Messaging

The purpose of this policy is to define the process to access the emails communication done by an employee.

4.1 Objective: The purpose of this policy is to define the process for the emails an employee.

4.2 Scope: This policy is applicable to all Company employees.

4.3 Email ID creation and deletion Process

- The Email-Id and profile of the newly joined staff (both teaching and non-teaching) shall be created within 10 days of receiving the Notification from the reporting Manager. Emails require employees of the SM Shetty shall be provided with a unique identity using his/her First Name and Last Name within 5 working days.
- The Email-Ids of the staffs who have resigned/ whose tenure has completed shall be deleted one month after receiving the Notification from the HR and reporting Manager
- The Email-Ids of the pass-out students shall be removed after two months of the declaration of result.
- Email accounts not used for 60 days will be deactivated and possibly deleted.
- Email ID Creation Form:

Bunts Sangha's S M Shetty Educational Institutions

Email Account Information

Requestor's Name: _____ Date: _____

Section: _____

Department: _____

HOD's Name: _____

Email Account Status

(Please select one of the following.)

Permanent ☐ Limited Time ☐ End Date _____

Requestor's Signature

(The requestor's signature is required.)

By signing this document, I signify that I have read, understand, and agree to abide by the Institute's IT policy.

Applicant's Signature: _____

HOD's Signature

(The HOD's signature is required.)

By signing this document, I signify that I have read, understand, and agree to abide by the Institute's IT policy.

HOD's Signature: _____

For Information Technology Dept. Use Only

Approved by: **Date:** **Time:**

Email ID created by: _____ **Date:** _____ **Time:** _____

Notification given by: _____ **Date:** _____ **Time:** _____

Please return this form to: Information Technology Dept.

Once created, all mail ID information will be sent to the applicant. Please allow three business days for email ID creation.

Created By IT Dept.

4.4 User Responsibilities: When using the email or messaging system users must at all times:

- Respect the privacy and personal rights of others;
- Use default settings and not make changes to the disclaimer (refer to Foot note for Standard format for a disclaimer at the end of this section)

Note: Email disclaimer

E-Mail Disclaimer Terms

The following terms shall apply to the recipients of the mails received from Bunts Sangha's S M Shetty Educational Institutions from the id – smshettyinstitute.org

Confidentiality

This email and any files transmitted with this email are confidential and intended solely for the use of the recipient to whom they are addressed. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this mail and attached file/s is strictly prohibited. You are also advised to notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system.

Warning - Transmission of viruses

Computer viruses can be transmitted via email. The recipient should check this email and attachments for the presence of viruses. Although the sender has taken reasonable precautions to ensure no viruses are present in this email, the sender shall not accept any liability / responsibility for any loss or damage arising from the use of this email or attachments.

- Strict use of email id provided by Institution for all official communication
- Take all reasonable care not to
    - plagiarize another person's work; or
    - defame another person;
- Not forward or otherwise copy a personal email (except with permission of the author) or an email which contains personal information or an opinion about a person whose identity is apparent (except with permission of that person);
- Not send forged messages, or obtain or use someone else's e-mail address or password without proper authorization;
- Not send mass distribution bulk messages and/or advertising without approval of the user's Head of Department, or Administrative Head;
- Not send SPAM. The user must ensure that the recipient(s) of the intended email have consented to receive such email(s);
- Not harass, intimidate or threaten another person/s;
- Not send sexually explicit material, even if it is believed that the receiver will not object. Remember, the intended receiver may not be the only person to access the communication
- Not send messages to more addressees unless necessary.
- Be careful when receiving e-mails from unknown senders. Do not open attachments and do not click on integrated links unless you are convinced that this e-mail is harmless.
- If you use Outlook Web Access (OWA), do not store passwords locally, and log out from the system as soon as you leave the computer.
- All email accounts maintained on our email systems are property of institute. Passwords should not be given to other people and should be changed once a month.

- In case of longer absence activate a meaningful absence note (auto-reply). Do not forward incoming mails automatically.
- All email including original messages, replies, and forwarded emails, should include an email signature with standard format at the end of the sender's text.

- Consultants will not be provided any email accounts. (Special Approval required for those consultants who require email)

4.5 Standards Required When Using Email

Appropriate standards of civility should be used when using e-mail and other messaging services to communicate with other staff members, students or any other message recipients. When using the email or messaging system users must not send:

- **Angry or Antagonistic Messages** – these can be perceived as bullying or threatening and may give rise to formal complaints under grievance procedures or discrimination / sexual harassment procedures; or
- **Offensive, Intimidating or Humiliating Emails** - Institution IT Resources must not be used to humiliate, intimidate or offend another person/s on the basis of their race, gender, or any other attribute prescribed under anti-discrimination legislation. Commonwealth and State laws and the Institution Equal Opportunity policy prohibit sexual harassment and discrimination, vilification or victimization on certain grounds such as race, gender, sexual preference, disability, or status as a parent or carer

4.6 Forwarding of Emails – Privacy and Ownership

S M Shetty Educational Institution owns copyright in all e-mail correspondence created by members of its staff in relation to their employment duties, excepting correspondence created by academic staff in respect to their research.

Copyright in work-related email will not be infringed by forwarding a message to another staff member or interested party (such as a consultant providing services to S M Shetty Educational Institution) on a need-to-know basis. However, care must be taken if an email contains **personal information**. "**Personal Information** means information or an opinion, whether true or not, about a person whose identity is apparent". This kind of information must not be forwarded or copied without prior permission from the person who is the subject of the personal information.

Copyright in a personal/non-work related e-mail belongs to the writer of the message. A personal e-mail must never be copied or forwarded without permission of the writer.

Copyright will be infringed if you send, without permission of the copyright owner, an audio or video file, music charts/lyrics, commercial photographs, journal article or report to another person using email.

Antivirus Policy

Antivirus software within institute, designed to protect the institutional resources against intrusion by Viruses & other malware (e.g.: worms, Trojans, adware, & malware). This standard defines antivirus standards on every computer including how often a virus scan is done, how often updates are done, which program will be used to detect and remove malware programs.

5.1 Objective: To device a high performance policy-based antivirus and content security administration for institute to protect the enterprise's network and system from virus attacks, worms, Internet-born email viruses and prevent

transmission of spam or non-business related contents.

5.2 Scope: This policy document is applicable to the systems, networks and devices within the institute Information Systems administrative domain.

5.3 Antivirus Policy for Desktop/Servers/Laptop: Every system (i.e. PC, Laptop, Servers etc.) must have anti-virus software installed, which has to be regularly updated with latest patches. This will be done automatically if you are connected to the update server. To ensure this take the help of IT team member or Local System Administrator in the respective region.

6 Password Policy

The purpose of this policy is to establish strong passwords, the protection of those passwords, & the frequency of change. To secure all data, applications, systems, and networks from unauthorized access.

6.1 Objective: To secure all data, applications, systems, and networks from unauthorized access.

6.2 Scope: This document will apply to all systems authenticating through domain controllers operated by Company or contracted with a third party by Company.

6.3 Creation: We will be using COMPLEX Password recommendations as per following guidelines, so the Passwords must meet complexity requirements as:

6.4 Initial Passwords: Any password created or changed by security administration, help desk, etc must be valid only for the user's initial login (set as expired). After providing the password, the user must be forced to change the Password before any other work can be done

6.5 Password Reuse: Validity of password is 90 Days and unique passwords must be selected without reusing any of the previous 2 passwords.

6.6 Password Management: Passwords must not be written and stored around the computer or desk area. Passwords to be kept under lock to be opened in case of emergency.

6.7 Password Sharing: Regardless of the circumstances, passwords must not be shared or revealed to anyone else besides the authorized users. To do so exposes the authorized user to responsibility for actions that the other party takes with the password. If users need to share computer resident data, they must use electronic mail, public directories on local area network servers, and other mechanisms.

6.8 Password Reset or Forgotten: Every time when password is reset on the request of User, the option for "change password at next logon"is enabled so that whenever the user logs on to the Domain system will force to change the password. We validate the user before resetting user password.

7 Desktop/Laptop/Device Policy

To protect the desktops& laptops from wide range of threats in order to ensure business continuity, minimizing business damages.

7.1 Objective: Desktop/Laptop needs to be suitable protected from wide range of threats in order to ensure

business continuity, minimizing business damages. This document presents a brief overview of institute Desktop security policy, guidelines and tips that should be followed while using Desktop. Once the laptop or desktops is issued will not be changed for 4 years.

7.2 Scope: This policy is applicable to all institute employees. It covers all Desktops& Laptops located on institute.

7.3 Installation: In institue, all the desktops and laptops in all the departments will be installed with following steps

- The entire desktop/Laptops are installed with Windows XP/Vista/Windows 7/higher Version Operating system along with all standard business software. HOD permission is required for specific software's likes AutoCAD, Third party software etc
- We follow naming convention guidelines while specifying the computer name, go through the naming convention Policy & guidelines.
- Operating System must be updated with the service pack (latest version available for operating system)
- All the local Administrative Passwords are up to Standard and already conveyed to team members.
- Administrator Password on the system.
- Make sure that all the existing data /User profile is deleted before issuing desktop/laptop to other

7.4 Exclusion / Exception for Local Admin Rights on Workstations: IT-Infra users are having Local admin Rights required as per their profile and business / work requirements as per policy. Other than IT users who need admin right, than proper approval from his/her HOD with proper justification is required before giving the admin rights. Admin Rights list is maintained which gets reviewed after every 6 months.

7.5 Local Admin right users Code of Conduct

- There should not be any unlicensed software installed on desktop/laptop apart from the standard software's provided by IT.
- Do not make any Interruption of services which disturb scheduled process like virus scan, windows update, and patch deployment.
- Do not download unwanted files leading to virus/spam.
- Do not copy infected Files.
- Do not keep inappropriate movies, pictures, games, songs in your desktop/laptop.
- Do not use CD/DVD/USB Storage Drives for personal usage.
- Do not delete any program files which may lead to OS Corruption.
- Do not add others to share their personal computer.
- Do not share drives/files/folder for others
- Do not change IP address/network properties.

7.6 Desktop, Laptop and Devices procurement Procedure: The Principal/ Chief Administrator /HOD are the sole authority for placing orders for IT software and hardware under IT team guidance. All IT related purchases will need to have full approval and authorization prior to requisitioning. All IT related hardware and software will be specified by SM Shetty IT and User or department is accountability for approval. Hardware and software cannot be purchased without approval by The Principal/ Chief Administrator /HOD of user.

7.6 Laptop Users:

- Laptops with bags are provided on basis of job requirement with HOD approval only.
- User is responsible for any Physical damage is found on laptop while returning the laptop.
- If Laptop bag is damaged Company will not provide any other bag.
- Company will not provide extra accessories like mouse, headphones, speakers, cooling Pads etc.

- Laptop user must fill the form with accuracy for getting laptop from IT dept.
- Laptop Handover form:

Created By IT

Bunts's Sangha's
S.M.Shetty Education Institutions

DECLARATION CUM UNDERTAKING

I, Shri/Miss…….. Received a company laptop for office use only with the following specification.

SR. NO.	User Name	Board	MAKE/MODEL	CPU	RAM	HDD	SERVICE TAG/SN	MAC Address	School Identification

I hereby give an undertaking that:

- **The laptop issued is for solely official purpose**
- **The employee shall be fully accountable for theft, loss or damage of the property**
- **The laptop requisition form has to be signed before taking possession of the laptop**
- **Employees may not take the laptop for repair to any external agency or vendor at any point of time**
- **I shall not bring in any illegal unauthorized software, Special software and install the same in my Laptop.**
- **I shall not make unauthorized copies of school's software by whatever means and take it out of the school premises or pass on to unauthorized person.**
- **I shall not make unauthorized copies of school's information and data by whatever means and pass it on to others without the approval of the management.**
- **I further give an undertaking that I shall take care to maintain the laptop in good working condition and return the laptop issued to me in good working condition as and when I resigned or retire from the school.**
- **I also giver an undertaking to reimburse the lost of the laptop is misplaced or lost by me.**

Name and Signature
Date:

Bunts Sangha's S M Shetty Educational Institutions | Page 1

8 File Server Access

This policy gives you and overview about how you can keep your critical & confidential data safe on our file server.

8.1 Objective: File Server is the System dedicated to Company Employees Data. One can keep his Critical and Confidential Data on File Server. Below mentioned Policy will help you out to Use your home folder on file server.

8.2 Description of Guidelines

- All computers, software and information are Company. Property and data in File Server, are considered as business information.
- Only Authorized personnel may access this service for either legal, maintenance or any other appropriate reason.
- The institute does not guarantee the privacy of data stored or transmitted on this system. The institute reserves every right to monitor, examine, block or delete any incoming or outgoing data in the institute's Network.
- By Default there is no Home Folder Assigned to Employee.
- A Generic Folder on File Server will be provided for your Team / Department.
- Institute's File Server applies regardless of the time of the day or day of the week
- Space of file server shared folder is 5GB only for each user
- Space of the common user folder is 2GB only.
- User must fill the form of "Shared Folder Creation Request Form" for file server folder creation.
- Folder Creation Request Form:

Confidential File Server 13-Jul-22

Bunts Sangha's S M Shetty Educational Institutions
Department Shared Folder Creation Request Form

In order to have employees within a department share files, General Manager A & A/ Principal/Vice Principal/Coordinator/HOD must fill out the form below to request the creation of a department shared folder and return it to IT dept. User will visit the IT department upon the completion of the creation of the shared folder in order to move the files selected to the new-shared folder and complete the setup process.

Important notes:

1. If any user listed below leaves the Bunts Sangha's S M Shetty Educational Institutions or moves to another department, please inform IT Dept. immediately, in order to have the permissions changed on the shared folder, if necessary.
2. General Manager A & A/Principal/Vice Principal/Coordinator/HOD must understand that the users granted Read/Write permissions will be able to delete, create, copy and modify any document in the department's shared folder.
3. Space of file server shared folder is 5GB only for each user.
4. Space of the common user folder is 2GB only.

Please fill clearly and accurately the required information below. All information requested must be entered for this form to be processed.

General Manager A & A/ Principal/Vice Principal/Coordinator/HOD

First Name: _____

Last Name: _____

Title: _____

Department:_____

Provide the Bunts Sangha's S M Shetty Educational Institutions usernames of all users authorized to access the shared folder and check either Read/Write or Read Only access:

Bunts Sangha's S M Shetty Educational Institutions User full Name	Department	Designation	Read/Write	Read Only

Access Authorization: I certify the above usernames are authorized to access my department networked shared folder and grant them permission to delete, create, copy and modify any and all files in the shared folder.

_____
General Manager A & A/ Principal/Vice Principal/Coordinator/HOD Signature

HR Dept. Information

Name: Designation:

Sign: _____

IT Dept. use only

Shared folder name: _____ Created date: _____

Server name folder was created on: _____ Creators name: _____

Group name assigned to folder: _____

9 IT Help desk

IT helpdesk is comprehensive help desk software that provides help desk agents and IT managers an integrated console to monitor and maintain the IT requests generated from the users of the IT resources in an institution. The IT help desk plays an important part in the provision of IT Services. It is very often the first contact the users have in their use of IT Help Desk when something does not work as expected. The IT help desk is a single point of contact for end-users who need help.

The two main focuses of the IT helpdesk are IT Request tracking. Using the following modules of Service Desk, technicians and system administrators can resolve issues of complex nature in no time and thus reduce the end-user frustration arising due to time consuming issue resolving process. They can also keep track of the needs of the institution with the help of asset management and proactively allocate resources to the right user/departments, thus increasing the productivity of the institution.

The following information gives details on the best way to contact the IT Help Desk team:

Normal business hours
Monday to Saturday 7:30am to 6:00pm
By phone 022-61327351, EXT 351
By email ithelpdesk@smshettyinstitute.org

Your call/email will be logged in to the IT Help Desk team queue and responded to in turn and within the response time state on IT Help Desk team. IT will then attempt to resolve the enquiry or fault by telephone or remote if possible, before arranging a site visit.

Service Level Agreement (SLA)

1) **High (SLA 4 Hours):** The priority of defect is set as high when the defect is affecting the software/Hardware or business severely. The system is unusable without the defect is fixed by IT team. (Example: Data center, Server, ISP, NVR, Mail server, Webserver etc.)

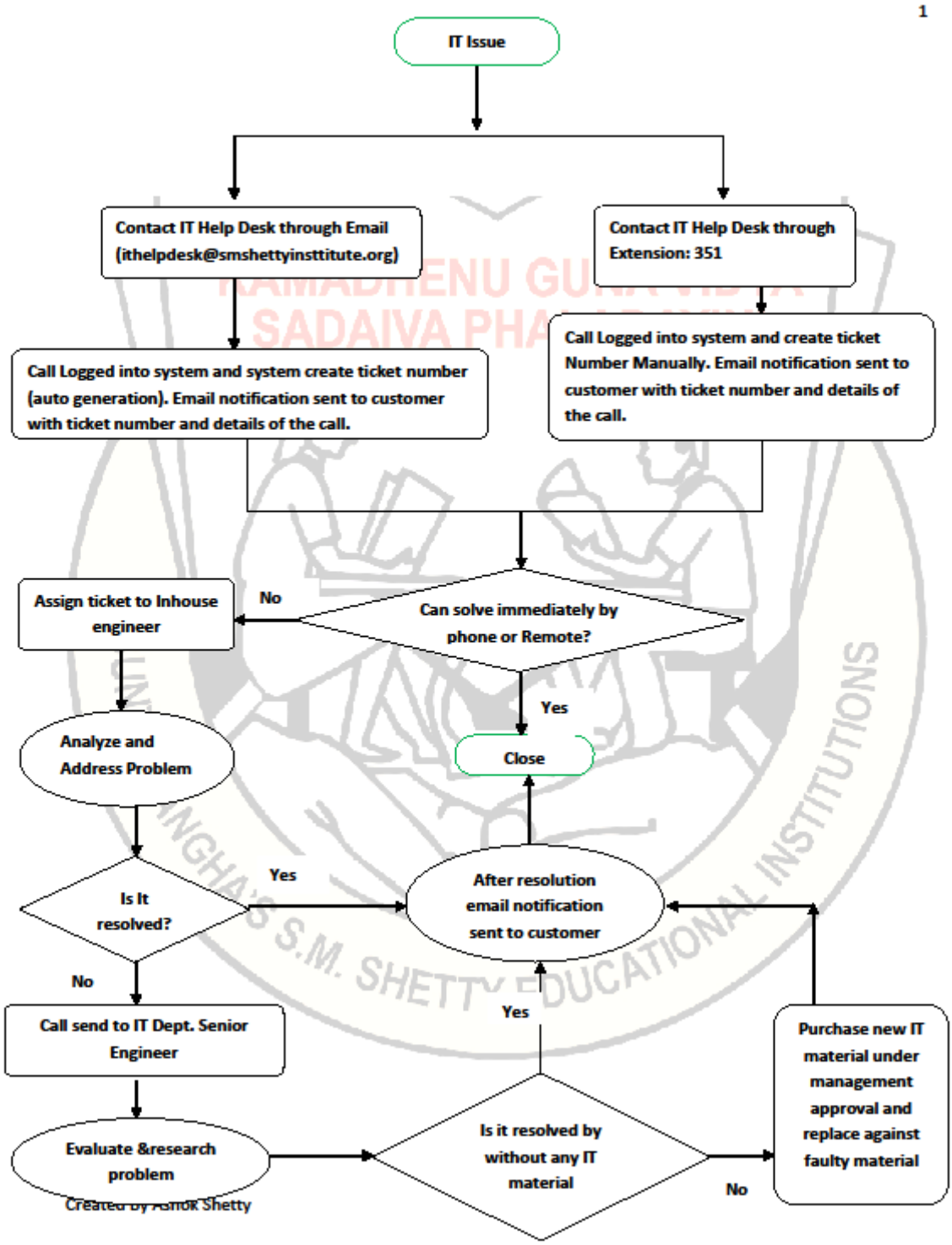
2) **Medium (SLA 8 Hours):** The priority of defect is set as medium when the defect can be fixed in normal course of Time. (Example: Repairing of PC, Projector, Printer, Scanner etc.)

3) **Normal (SLA 1 Day):** The priority of the defect is set as normal when very minimal impact on the current system. (Example: Website update, Projector setting, PC formatting, CCTV repairs etc.)

4) **Low(SLA 3 Days):** The priority of the defect is set as low when the defect is an irritant and can be fixed later after more serious defects (Example: keyboard, Mouse, Windows update, Antivirus update, Lab compliance etc.)

Service Level Agreements (SLA) of IT helpdesk	
Name	**Resolution Time**
High	0Days 4Hrs 0Mins
Medium	0Days 8Hrs 0Mins
Normal	1Day 0Hrs 0Mins
Low	3Days 0Hrs 0Mins

See below the process of what happens when you have an IT Support Issue.


1
IT Issue
Contact IT Help Desk through Email (ithelpdesk@smshettyinsttitute.org)
Contact IT Help Desk through Extension: 351
Call Logged into system and system create ticket number (auto generation). Email notification sent to customer with ticket number and details of the call.
Call Logged into system and create ticket Number Manually. Email notification sent to customer with ticket number and details of the call.
Can solve immediately by phone or Remote?
No
Assign ticket to Inhouse engineer
Yes
Close
Analyze and Address Problem
Is It resolved?
Yes
After resolution email notification sent to customer
No
Call send to IT Dept. Senior Engineer
Yes
Evaluate &research problem
Is it resolved by without any IT material
No
Purchase new IT material under management approval and replace against faulty material
Created by Ashok Shetty

10 Security of Information technology Resources and Data

10.1 Authorized User's Responsibilities

Authorized Users have a responsibility at all times to:

- Act lawfully;
- Keep all Institutions IT Resources secure and to observe the Institutions IT Security Policy;
- Not compromise or attempt to compromise the security of any IT Resource belonging to the Institution or other institutions or individuals, nor exploit or attempt to exploit any security deficiency.
- Take reasonable steps to ensure physical protection including damage from improper use, food and drink spillage, electrical power management, anti-static measures, protection from theft, and sound magnetic media practices;
- Ensure their computers are not left unattended without first logging-out and/or securing the entrance to the work area – particularly if the computer system to which they are connected contains sensitive or valuable information.

10.2 Records Management

Authorized Users are required at all times to:

- Take reasonable steps to ensure that important Institution data is stored appropriately on S M Shetty Educational servers for preservation and backup;
- Domain controller(PDC) and additional domain controller(BDC) with replication for no downtime
- File server data backup sync with NAS1 storage and NAS1 storage sync with NAS2 and cloud backup
- CCTV data sync with NVR and stored 25 to 30 days backup for view
- Ensure course materials are placed on official S M Shetty Educational Institutions servers;
- Ensure course materials are not placed on personal web pages or servers; and
- Observe appropriate Institution record management protocols such as the Electronic Mail Recordkeeping Protocol.
-

10.3 Confidential Information

Authorized Users have a duty to keep confidential:

- All Institution data unless the information has been approved for external publication; and
- Information provided in confidence to the Institution by other entities.

Each staff member is under a duty not to disclose Institution business information unless authorized to do so. Breach of confidentiality through accidental or negligent disclosure may expose a User to disciplinary action.

10.4 Personal Information

Personal information about an individual, including personal information that is also Health Information, must not be disclosed without consent of the individual concerned. However, Privacy legislation does provide for release of personal information without consent in certain circumstances e.g. where the information is requested by the police or where the Institution has reason to suspect that unlawful activity has been, or is being engaged in, such as intentional infringement of copyright. A decision on the legality of disclosure in the particular circumstances must be made by the Institution's Privacy Officer or the Institution Solicitor's Office.

10.5 Cyber security (Sophos Firewall)

Cyber security consists of technologies, processes and measures that are designed to protect systems, networks and data from cyber-crimes. There are various methods through which the crime is penetrated into the computer, network, hardware, software or in your cell phone.

- Unauthorized access: Unauthorized access also known as cracking as opposed to hacking, means gaining access to a system without permission of the users or without proper authority. This is generally done either by fake identity, or by cracking access codes.
- E-mail bombing: This means sending a large number of mails to the victim resulting in the victims mail account (in case of individual) or server (in case of corporations) crashing.
- Data diddling: This kind of attack involves altering the raw data before it is processed by a system and re-altering it after processing.
- Virus/Worm attack: A virus is a program, which attaches itself to another file or a system and then circulates to other files and to other computers via a network. They usually affect computers by either altering or deleting data from it. Worms on the other hand do not interfere with data. They simply multiply until they fill all available space on the computer.
- Trojan attack : A Trojan is a program, which appears to be something useful but under the disguise of a useful program causes some damage
- Pharming: It is an attempt to defraud Internet surfers by hijacking a Web site's domain name, or URL, and redirecting users to an imposture Web site where fraudulent requests for information are made.

Cyber-crime prevention

Practices recommended for cyber-crime prevention is always better than cure. It is always better to take certain precaution while operating the net.

- Firewalls: These are programs, which protect a user from unauthorized access attacks while on a network. They provide access to only known users, or people who the user permits.
- Frequent password changing: With the advent of multi-user systems, security has become dependent on passwords. Thus one should always keep passwords to sensitive data secure. Changing them frequently and keeping them sufficiently complex in the first place can do this.
- Safe surfing: Safe surfing involves keeping ones e-mail address private, not chatting on open systems, which do not have adequate protection methods, visiting secure sites. Accepting data from only known users, downloading carefully, and then from known sites also minimizes risk
- Frequent virus checks: One should frequently check ones computer for viruses and worms. Also any external media such as floppy disks and CD ROMS should always be virus checked before running.

- Email filters: These are programs, which monitor the inflow of mails to the inbox and delete automatically any suspicious or useless mails thus reducing the chances of being bombed or spoofed.
- Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
- Always keep back up volumes so that one may not suffer data loss in case of virus contamination
- Never send your credit card number to any site that is not secured, to guard against frauds.
- Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.
- Disconnect from internet when not in use.
- Habitually download security protection update patches & Keep your browser and operating system up to date.
- Change administrator's password from the default password. If the wireless network does not have a default password, create one and use it to protect the network.
- Disable file sharing on computers.
- Turn off the network during extended periods of non-use, etc.
- Use a variety of passwords, not same for all of your account.
- Never respond to text messages from someone you don't know.
- Open email attachment carefully.

10.6 Institution Liability

The Institution accepts no responsibility for:

- Loss or damage or consequential loss or damage, arising from the use of the Institution's IT Resources.
- Loss of data or interference with files arising from the Institution's efforts to maintain the IT Resources.

11 Prohibited use of Information Technology Resources and Possible Consequences

11.1 S M Shetty Educational Institutions Name, Crest and Logo

The S M Shetty Educational Institutions Name, crest or logo may only be used with prior approval from the Office of Chief Administrator.

11.2 Advertising and Sponsorship

Paid advertisements are not permitted on any website using a S M Shetty Educational Institutions domain name, personal website or any website, which has a substantial connection with the Institution (such as a website for a research program) except with the written permission of the Principal / Administrative Head.

11.3 No Business Activities

Authorized users are not permitted to run a business or publish a non-S M Shetty Educational journal/magazine (unless prior written authorization has been obtained from the Institution) on institutes IT Resources. Users must not publish their Institutes e-mail address on a private business card.

11.4 Unauthorized Access

Authorized users are expressly forbidden from unauthorized access or attempting to gain unauthorized access to IT Resources belonging to other institutions.

11.5 Infringement of Copyright

Authorized users are expressly forbidden to engage in any of the conduct described in the Schedule as infringing conduct.

11.6 Databases, online journals, eBooks

Use of electronic resources provided by the Institution is governed by individual licence agreements and is for non-commercial research and study purposes only. Users are required to comply with use restrictions set out on the specific site or stated in the licence agreement, and must not systematically download, distribute or retain substantial portions of information. Using software, including, scripts, agents or robots is prohibited and may result in loss of access to the resource for the whole S M Shetty Educational Institutions community.

Any use of electronic resources for teaching purposes must comply with the contractual terms of use of the electronic resource from which the material was sourced.

11.7 Peer to Peer File Sharing

Installation or use of peer to peer file sharing software s is not permitted on the Institutions network. Exceptions for legitimate teaching or research use must be approved by the Head of School or equivalent, and only where no alternative technology is appropriate.

11.8 Pornography

Authorized users are not permitted to utilize the Institution's IT Resources to access pornographic material or to create, store or distribute pornographic material of any type.

11.9 Gambling

Authorized users are not permitted to utilize the Institution's IT Resources to gamble.

11.10 Possible Consequences

11.10.1 For S M Shetty Educational Institution's Staff

Staff found to have breached this policy will be subject to disciplinary action in accordance with the disciplinary procedure. Criminal offences will be reported to the police.

11.10.2 Authorized Users Other Than Institution Staff

Authorized users (other than S M Shetty Educational Institution staff) found to have breached this policy may be subject to appropriate action as determined by the Institution. Such action may include but is not limited to; sanctions and/or removal of access to S M Shetty Educational Institution IT Resources. Criminal offences will be reported to the police.

12 Privacy and Surveillance

12.1 Security and Privacy

The accounts, files and stored data including, but not limited to, e-mail messages belonging to users at the Institution are normally held private and secure from intervention by other users, including the IT staff.

There are situations in which duly authorized IT staff may be required to intervene in user accounts, temporarily suspend account access or disconnect computers from the network in the course of maintaining the Institution's IT Resources such as repairing, upgrading or restoring file servers or personal computer systems.

Users should be aware that IT staff may from time to time become aware of the contents of user directories and hard disk drives in the normal course of their work, and they are bound to keep this information confidential.

12.2 Access to and Monitoring

The Institution does not generally monitor e-mail, files or data stored on Institution IT resources or traversing the Institution network. However, the Institution reserves the right to access and monitor any computer or other electronic device connected to the S M Shetty Educational Institution network. This includes equipment owned by the Institution and personal computing equipment (e.g. laptops) that are connected to the network.

Access to and monitoring of equipment is permitted for any reason, including but not limited to, suspected breaches by the user of his/her duties as a staff member, unlawful activities or breaches of Institution legislation and policies. Access to and monitoring includes, but is not limited to e-mail, web sites, server logs and electronic files.

The Institution may keep a record of any monitoring or investigations.

12.2 Prior Approval Required

Prior approval must be obtained from the Chief Administrator, Human Resources Division (or nominee), before a user's e-mail, files or data may be accessed by authorized staff. Any information obtained under this approval will be treated as confidential, and only disclosed to relevant 3rd parties. Access to the information will be strictly on a need-to-know basis.

12 Relevant Indian Legislation, Policies and Associated Documentation

Users need to be aware of conduct which may breach laws outside of the Institution and lead to criminal or civil proceedings and / or penalties for which they will be held personally accountable.

12.1 Copyright

Text (including song lyrics), computer programs, illustrations (including maps and diagrams) photographs, music recordings, videos, films and television broadcasts are all protected by copyright. The duration of copyright protection is generally 70 years following the death of the author. A user must not copy, send or place materials on the web without permission from the copyright owner, unless a relevant exception under the Copyright Act applies. Infringement of another person's copyright could result in personal liability for damages.

Users should assume that all materials published on the web are in copyright, unless explicitly stated otherwise. If a user wishes to include material from another webpage in one of their own pages, they should create a hypertext link pointing to the material rather than copy it.

12.2 Trade Marks

A user must not copy a trade mark or logo belonging to another party. Trade mark infringement will expose the user to liability for damages.

12.3 Competition and Consumer Legislation

Competition and consumer legislation contains provisions which prohibit passing off and misleading and deceptive conduct. If a user were to copy material from an external site onto a Institutions website (including features such as logos and trademarks) so that persons accessing the website would believe that Institutions had been authorized to carry the material, this would constitute passing off or deceptive or misleading conduct.

12.4 Spam

Users must not send unsolicited commercial electronic messages. Any commercial messages that are sent electronically (including email, instant messaging or telephone accounts) must include information about the individual or institution who authorized the sending of the message and a functional unsubscribe facility.

12.5 Anti-discrimination

Laws and the Institution prohibit sexual harassment and discrimination, vilification or victimization on grounds such as race, gender, sexual preference, disability, or status as a parent or carer. Institution IT facilities must not be used to humiliate, intimidate or offend others on the basis of their race, gender, or any other attribute prescribed under anti-discrimination legislation.

12.6 Defamation

A user should not publish a statement about another person which could harm that other person's reputation. There is no need for the person to have been named specifically if he/she can reasonably be identified. Photographs and cartoons can also be defamatory if they hold someone up to ridicule or contempt. In a defamation case, truth is not always a defence.

.

Section III - Do's & Don't's

1. Mailbox Management

Individuals are expected to treat their mailbox like an electronic in-tray, ensuring that it is regularly checked and that messages requiring further action are dealt with promptly – including sending holding responses where appropriate. Periodically remove the unwanted mail from outlook items.

2. Use of Email

Staff must take care with any suspected malicious or nuisance e-mails received (e.g. chain e-mail, hoax and spam e-mails) and delete them. If any suspicious e-mails are received they should be reported to the IT Help Desk.

Individuals must never open attachments to an e-mail of unknown origin as they may contain viruses and other malware.

3. Downloading of Information from the Internet

Individuals must not download non-work related information from the Internet. To reduce the likelihood of a virus infection, individuals must take care to ensure that the files are from a trustworthy source.

Individuals requiring any new software, including any plug-ins, must make a formal request to the IT Service Desk (Ext 351).

Software must not be downloaded and/or installed onto School IT equipment unless it has been approved by the Dept Head/IT-Head and can be validated that it is licensed for current use.

Graphical, audio and video files may be downloaded and stored on School network for Official use only.

Individuals are reminded that copyright laws apply to the Internet and care must be taken should there be a need to re-use any information (including images) in any School work (Refer to 7.1 above)

4. Uploading Data / Information on Internet

Any users who are responsible for uploading data / information to the Internet must be sure that the information being uploaded is suitable to upload.

5. Acceptable Use of Internet

For Students & Teachers

- Internet sessions will always be supervised by a teacher.
- Filtering software and/or equivalent systems will be used in order to minimize the risk of exposure to inappropriate material.

- The school will regularly monitor pupils' Internet usage.
- Uploading and downloading of non-approved software will not be permitted
- Virus protection software will be used and updated on a regular basis.
- The use of personal pen drives or CD-ROMs in school requires a teacher's permission.
- Students will observe good "netiquette" (i.e., etiquette on the Internet) at all times and will not undertake any actions that may bring the school into disrepute.

For Teachers

- When you download YouTube online study material/software it is stored in the server hard disk. The same can be used for further teaching, this will be beneficial to save time on online browsing & internet speed.
- One common login will be created for teacher to use in all classrooms. No student login will be given.
- Teacher can access the common folder for sharing the data of study material.
- Shifting of IT-Resources from one location to another location should be done with prior permission of the concerned authority.

Students should NOT

- Use any device that is logged on by another user
- Deliberately mess with and/ or delete another person's files
- Use social media during the school day
- Send, create or publish anything which others might reasonably find offensive
- Use mobile phone, cameras or other electronic devices to take, publish or circulate pictures or videos of anyone without their permission.
- Try to look at unsuitable material such as pornographic, racist or offensive material. Such an act is strictly forbidden and may lead to prosecution by the police
- Deliberately damage the network or other electronic equipment by means of harmful files or programs (eg. Virus infections, malware etc.), hacking or physical tampering.

Employees should NOT

- Allow another person to use the computer under their login.
- Add, modify, repair, reconfigure or otherwise tamper with any device on the network infrastructure including, but not limited to: wireless network devices, computers, printers, servers, cabling, switches/hubs, routers, etc.
- Destroying or tamper with any computer equipment or software.
- Make use of any "hacking tools" that can be used for "computer hacking" or run or load on any computer system.
- Make use of school computers for illegal activities including but not limited to planting viruses, hacking, or attempted unauthorized access to any system.
- Violate any state law or regulation, board policy or administrative rule.

6. Computer Security

6.1 Data Storage

Access to individual data areas will only be granted following a written approval from the "owners" of that area.

Storage of data on PC or Laptop's C: drive is discouraged and all users are requested not to store files on PC or Laptop's C:\drives because in the event of failure, all data stored on the C: drive would be lost as it not backed up,

All information related to School is to be stored on the personal network drive or on School shared drives.This is a secure storage area which is regularly backed up and is therefore resilient to failure.

The following types of file can only be stored if they relate to explicit School needs.

File Type Description
.AVI Movie Files; .MPG Movie Files; .MPEG Movie Files
.MP3 Sound Files ;.MP4 Sound Files;.M4A ITunes Files
.MOV Movie Files;.EXE Executable files1;. SCRScreen Savers

6.2 Passwords

Passwords given to you are for your use only.

Passwords should not be written down or given to others to use under any circumstances.

If your manager or Dept. Head needs access to your computer, for example if you are off sick, they must contact the IT Service Desk to request managerial access to your computer.

6.3 Viruses

All files received on disc from outside the School or received via electronic mail must be checked for viruses before being used on School equipment. You must not intentionally introduce/send or download files or attachments which contain viruses, or which are meant to compromise the School systems.

If a virus is suspected, the IT Service Desk must be informed immediately. The workstation should not be used until given permission from the IT Service Desk and a sign stating this should be placed on the workstation to warn other users. Any disks, CD ROMS, and USB memory sticks that have been used on the suspected infected workstation should be gathered together and not used.

6.4 Printing

Staff must ensure adequate care is taken when printing information, utilising the use of School secure printing solution. If there is a printer fault when printing **OFFICIAL** or **OFFICIAL-SENSITIVE** material please phone the IT service desk who will ensure that any unprinted files are deleted from the print queue.

Save paper. Print only if needed.

6.5 Scanning

Staff must ensure adequate care is taken when scanning documents and using School secure scanning solution. Checking the destination file or email address.

Policy Exception:

For any policy exception above mentioned IT department will seek the justification from HOD of the Concerned department an also IT Department will evaluate the permission on case to case basis. If the exception list exceeds, this needs to by approve by the Chief Administrator/Principal.

Policy Violation:

All the employees & consultants those who failure to adhere to the above mentioned policies shall lead to Disciplinary action