



---

## IT Policy

---

2017

---

<b>Document Name:</b>	IT Policy		
<b>Document ID:</b>	IT/2017/ver1.0	<b>Version:</b>	1.0
<b>Prepared by:</b>	D Bahl	Dir.(IT)	<b>Date:</b> 15/5/2017

## 1. Preface

- 1.1. Information security is a process by which an organization protects and secures information, systems, media and facilities that process and maintain information vital to its operations. Any unauthorized as well as accidental misuse of information or information system may result in financial loss, business loss, damaged reputation, improper disclosure, lawsuits and non-compliance with the regulatory provisions etc. Owing to the growth in the use of IT and IT based applications in day-to-day operations of the Group, the need for putting in place security controls has been felt.
- 1.2. This IT security Handbook and Manual consists of security policies and guidelines and security organization structure for Management of risk through prudent business practices and use of appropriate security mechanism.
- 1.3. This Manual describes the Information Security Mechanism of Rayat Bahra Group (Organization). It is designed to ensure that all requirements relating to Information Security are recognized and consistent and uniform implementation of security control measures is maintained.

## 2. Purpose

- 2.1. The purpose of this policy is to outline rules concerning sensitivity of Information & the acceptable use of computer equipment in the Organization. These rules are in place to protect the employee and students of the Organization. Inappropriate use exposes the Group to risks including virus attacks, compromise of network systems and services, and legal issues.
- 2.2. To protect and safeguard all critical information and information processing assets in order to ensure provision of services and business continuity. This includes (but not limited to) electronic/ print information etc on servers, workstations, laptops, networking and communication devices, CDs, removable drives and information printed or written on paper or transmitted by facsimile or any other medium.

## 3. Applicability

- 3.1. This policy manual applies to all employees & students of the Group and third parties engaged by Group, including, but not limited to, consultants, contractors, vendors and third parties (Security staff, housekeeping, Office attendants etc.)
- 3.2. This policy applies to all equipment that is owned or leased by Organization.

## 4. Enforcement

Any employee, student found to have violated the policy may be subject to disciplinary action.

## 5. IT Policy

- 5.1. Acceptable Use Policy** (Annexure I)  
Defines how users may use IT computer resources.
- 5.2. Password Policy** (Annexure II)  
This policy Defines minimum and maximum length of passwords, password complexity, how often it must be changed. It also defines how many bad login attempts over what specific amount of time will cause an account to be locked.
- 5.3. Internet Connection Policy** (Annexure III)  
This Policy specifies how users are allowed to connect to the internet and provides for IT department approval of all connections to the internet. Requires all connections to be approved by the IT department and what is typically required for approval such as the operation of a firewall to protect the connection. Also defines how the network will be protected to prevent users from going to malicious web sites. Defines whether user activity on the network will be logged and to what extent. Specifies what system will be used to prevent unauthorized viewing of sites and what system will log internet usage activity.
- 5.4. Anti-virus and Malware Policy** (Annexure IV)  
This policy defines anti-virus policy on every computer including how often a virus scan is done, how often updates are done. Defines what programs will be used to detect, prevent, and remove malware programs. It also defines what types of files attachments are blocked at the mail server. It also specify how files can enter the trusted network and how t hese files will be checked for hostile or unwanted content. For example it may specify that files sent to the enterprise from outside the trusted network be scanned for viruses by a specific program.
- 5.5. Asset control policy** (Annexure V)  
Defines how assets such as computers are tracked. This policy will allow the locations and users of all assets to be tracked. This policy will define a property move procedure. This policy will define what must be done when a piece of property is moved from one building to another or one location to another. It will define who signs off on the movement of the property. This will allow the database to be updated so the location of all computer equipment is known. This policy will help network administrators protect the network since they will know what user and computer is at what station in the case of a worm infecting the network. This policy must also cover the fact that data on the computer being moved between secure facilities may be sensitive and must be encrypted during the move.

- 5.6. Email & Communication Policy** (Annexure VI)  
The purpose of this policy is to ensure the proper use of Group's email system and make users aware of what Group deems as acceptable and unacceptable use of its email system.
- 5.7. Backup Policy** (Annexure VII)  
This policy is designed to protect data in the organization to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.
- 5.8. Information Sensitivity Policy** (Annexure VIII)  
The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Group without proper authorization.
- 5.9. Removable Media Policy** (Annexure IX)  
The policy establishes the principles and working practices that are to be adopted by all users in order for data to be safely stored and transferred on removable media.

## 6. Security Organization

### 6.1. Security Committee

The Security Committee is the highest body for Information Security in the organization. The composition of Committee is as under:

1. Group Chairman
2. VC/Campus Director or their Nominee
3. Director IT (CIO)

Other members may be co-opted as required. Security Committee shall be responsible for:

1. Periodic Review of security environment and controls.
2. Developing and maintaining Business Continuity Plan.
3. Review and approval of Risk Assessment
4. Approve major initiatives to enhance information security.

### 6.2. Organization Security Setup

The Security set shall be composed of

- a) Director (IT)
- b) Registrar / Campus Administrative Officer
- c) Campus IT Administrator
- d) Campus IT Technicians
  - a. Networking Technicians
  - b. Hardware Engineers

### 6.3. Responsibilities

#### 6.4. Responsibility of Director(IT)

- 6.4.1. Will be the Security Committees representative for information security and will ensure implementation of the information security policy and procedures on its behalf.
- 6.4.2. Briefing the Selection Committee on current threats and recommended safeguards.
- 6.4.3. Reporting to the management forum on the progress within the framework, incidents, security status, and current threats.
- 6.4.4. Ensure appropriate handling of all security incidents and initiate/recommend suitable corrective and preventive measures.
- 6.4.5. Will be the Member – Secretary of the Security Committee and will organize meetings of the Committee with Chairman’s approval.
- 6.4.6. Will derive assistance from Registrar/Campus Administrative Officer designated Security & IT Engineers for implementing agreed security measures

#### 6.5. Responsibility of Registrar/Campus Administrative Officer

- 6.5.1. Ensure employees & Students are aware of their rights and duties with respect to use of organizations computing resources and networks. The

computing resources are the property of the organization and to be used for business purposes only.

- 6.5.2. Create Sensitivity Guidelines in Human Resource Manual as per sensitivity Policy for Classification of Information into Group Public & Group Confidential, Create rules for distribution/disposal/assess of the information and make employees aware of the same.
- 6.5.3. Create & Finalize rules regarding entitlement of mobile computing equipment (Laptops, Palmtops etc).
- 6.5.4. Create a culture that promotes compliance, encourages employees to raise their security questions and concerns, and prohibits retribution.

#### **6.6. Responsibility of Campus IT Administrator**

- 6.6.1. Administer AD, Domain Controller
- 6.6.2. Administer & Monitors UTM and implements all security policies
- 6.6.3. Administer Employees of all Categories and implements the Internet related policies applicable on them
- 6.6.4. Receipt of Internet Access Request Forms, file the same
- 6.6.5. Create , Edit and delete Users
- 6.6.6. Maintain Mantis / comparable Software for complaint logging
- 6.6.7. Ensure appropriate handling of all security incidents at the designated site and initiate suitable corrective and preventive measures.
- 6.6.8. Ensure compliance with Intellectual Property Rights (IPR) so that no un-licensed software is used within their location.
- 6.6.9. Compile Summary of IT Technicians Action Taken Report
- 6.6.10. Compile Incidents of Security Threats, Data pilferage & Theft and other security issues
- 6.6.11. Action Taken report to be prepared and sent to Director(IT)/ Concerned Dean/Registrar/Campus Administrative Officer on a weekly basis.

#### **6.7. Responsibilities of Campus IT Technicians**

- 6.7.1. Report to Campus IT Administrator
- 6.7.2. Closing of Complaints forwarded to them by Campus IT Administrator
- 6.7.3. Report on weekly basis to Campus IT Administrator, No of complaints received, attended, resolved and pending. Complaints relate to networking, Hardware, software.

#### **6.8. Employees Responsibilities**

All employees are expected to follow the general guidelines below to ensure information security for the organization:

- 6.8.1. Comply with the security policy and
- 6.8.2. Ensure that any user-id, password or any other device issued for accessing Group resources remains confidential and under the employee's control.
- 6.8.3. Access only the specific information required for doing the job.
- 6.8.4. Limit or restrict use of the internet, email as per entitlement.
- 6.8.5. Take precautions for any comments made publicly or sent electronically.

- 6.8.6. Comply with software license agreements when using copyrighted software.
- 6.8.7. Promptly report any concerns about security exposures or possible violations of policy/ procedures.

(Annexure I)

## Acceptable Use Policy

### 1. Overview

Effective security is a team effort involving the participation and support of every Group employee who deals with information and/or information systems. It is the responsibility of every computer user/lab technician to know these guidelines, and to conduct their activities accordingly.

### 2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Group. These rules are in place to protect the employee and Group. Inappropriate use exposes Group to risks including virus attacks, compromise of network systems and services, and legal issues.

### 3. Scope

This policy applies to all equipment that is owned or leased by Group.

### 4. Policy

#### 4.1. Creation of Active Directory and Domain

- 4.1.1. Campus IT department to maintain server with Active Directory, DHCP and DNS role. All systems used by employees should be connected to Domain. Every system shall have a Admin Password which shall be maintained by Respective IT Department of the Campus.

#### 4.2. General Use and Ownership

- 4.2.1. While it is the intention of Group to provide a reasonable level of privacy, users should be aware that the data they create on the systems remains the property of Group.
- 4.2.2. Because of the need to protect Group network, management cannot guarantee the confidentiality of personal information stored on any device belonging to Group.
- 4.2.3. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. In there is any uncertainty, employees should consult their IT Department
- 4.2.4. For security and network maintenance purposes, authorized IT Staff within Group may monitor equipment, systems, emails, files and network traffic at any time.
- 4.2.5. Group reserves the right to audit systems on a periodic basis to ensure compliance with this policy.



### 4.3. Security and Proprietary Information

- 4.3.1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- 4.3.2. Because information contained on portable computers is especially vulnerable, special care should be exercised while handling Laptops.
- 4.3.3. Postings by employees from a Group email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Group, unless posting is in the course of duties.**
- 4.3.4. All hosts used by the employee that are connected to the Group Internet/Intranet, whether owned by the employee or Group, shall be continually executing approved virus-scanning.
- 4.3.5. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

### 4.4. Unacceptable Use

Under no circumstances is an employee of Group authorized to engage in any activity that is illegal under local, state, central or international law while utilizing –Group owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

#### 4.4.1. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or Company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Group.
2. Unauthorized copying of copyrighted material and the installation of any copyrighted software for which Group or the end user does not have an active license is strictly prohibited.
3. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
4. Revealing your account password to others or allowing use of your account by others. This includes family and other household.
5. Using a Group computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
6. Making fraudulent originating from any Group account.

7. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
8. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
9. Circumventing user authentication or security of any host, network or account.
10. Providing information about group employees to parties outside Group.

#### **4.4.2. Blogging**

1. Blogging by employees, whether using Group's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Groups' systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, is not detrimental to Group's best interests, and does not interfere with an employee's regular work duties.
2. Employees are prohibited from revealing any confidential or proprietary information/ or any other material when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Group and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging.
4. Employees may also not attribute personal statements, opinions or beliefs to Group when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of group. Employees assume any and all risk associated with blogging.

## Password Policy

### 1. Overview

All group systems should be on domain controller. Employees and personnel that have access to Group computer systems & domain must adhere to the password policies defined below in order to protect the security of the network, protect data integrity, and protect computer systems.

### 2. Purpose

This policy is designed to protect the Group resources on the network by requiring strong passwords along with protection of these passwords, and establishing a minimum time between changes to passwords.

### 3. Scope

This policy applies to any and all personnel who have any form of computer account requiring a password on the Group network

### 4. Password Protection

- a) Never write passwords down. If passwords are to be written, then they should be kept at a secured place.
- b) Never send a password through email.
- c) Never reveal your password over the telephone.
- d) Never include a password in a non-encrypted stored document.
- e) Never tell anyone/share your password.
- f) Never hint at the format of your password.
- g) Never reveal or hint at your password on a form on the internet.
- h) Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program.
- i) Never use your corporate or network password on an account over the internet which does not have a secure login where the web browser address starts with https:// rather than http://
- j) Report any suspicion of your password being broken to your IT Department
- k) Don't use common acronyms as part of your password.
- l) Don't use common words or reverse spelling of words in part of your password.
- m) Don't use names of known people or places as part of your password.
- n) Don't use part of your login name in your password.
- o) Don't use parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses.
- p) Be careful about letting someone see you type your password.

## 5. Password Requirements (subject to change)

Those setting password requirements must remember that making the password rules too difficult may actually decrease security if users decide the rules are impossible or too difficult to meet. If passwords are changed too often, users may tend to write them down or make their password a variant of an old password which an attacker with the old password could guess. The following password requirements will be set by the respective IT Departments:

- a) Minimum Length - 8 characters recommended
- b) Maximum Length - 14 characters
- c) Minimum complexity - Passwords should use three of four of the following four types of characters:
  - d) Lowercase
  - e) Uppercase
  - f) Numbers
  - g) Special characters such as !@#\$%^&\*(){}[]
- h) Passwords are case sensitive and the user name or login ID is not case sensitive.
- i) Password history - Require a number of unique passwords before an old password may be reused. This number should be no less than 8.
- j) Maximum password age - 60 days
- k) Minimum password age - 2 days
- l) Reset account lockout after - The time it takes between bad login attempts before the count of bad login attempts is cleared. The recommended value is 20 minutes. This means if there are three bad attempts in 20 minutes, the account would be locked.
- m) Account lockout duration - Some experts recommend that the administrator reset the account lockout so they are aware of possible break in attempts on the network. However this will cause a great deal of additional help desk calls. Therefore depending on the situation, the account lockout should be between 30 minutes and 2 hours.
- n) Password protected screen savers should be enabled and should protect the computer within 5 minutes of user inactivity. Computers should not be unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked. they can press the CTRL-ALT-DEL keys and select "Lock Computer".

## 6. Other Considerations

Administrator passwords should be protected very carefully. Administrator accounts should have the minimum access to perform their function. Administrator accounts should not be shared.

## Internet Usage Policy

### 1. Overview

1.1. This internet connection policy requires users to use the internet for office purposes only and requires users to avoid going to malicious web sites which could compromise security. The policy defines that internet activity while connected to the network may be logged and monitored. It specifies what system will be used to prevent unauthorized viewing of sites and what system will log internet usage activity. It defines how the network will be protected to prevent users from going to malicious and banned web sites.

### 2. Purpose

2.1. This policy is designed to protect the Group's resources against intrusion by malware that may be brought into the network by users as they use the internet. It is also designed to prevent unauthorized and unprotected connections to the internet which may allow a host of unsafe content to enter the Group's network and compromise data integrity and system security across the entire network.

### 3. Scope

3.1. The Internet usage Policy applies to all Internet users (employees including permanent full-time and part -time employees, students, contract workers, temporary agency workers, business partners, and vendors) who access the Internet through the computing or networking resources. The company's Internet users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Internet services.

#### 3.2. Internet Services Allowed

Internet access is to be used for business purposes only. Following Internet services will be provided to users as needed:

- E-mail -- Send/receive Email mail messages to/from the Internet (with or without document attachments). – Annexure Email and Communication Policy – Annexure VII
- Navigation -- WWW services as necessary for business purposes, using a hypertext transfer protocol (HTTP) browser tool.
- File Transfer Protocol (FTP) -- Send data/files and receive as necessary for business purposes.
- Telnet -- Standard Internet protocol for terminal emulation.

#### 3.3. Request & Approval Procedures

##### 3.3.1. Request for Internet Access

Internet access will be provided to users to support business activities and only as needed to perform their jobs. As part of the Internet access request process, the employee/student is required to read IT Security Handbook and Manual. The

user must then sign the statements (located on the last page of each document) that he/she understands and agrees to comply with the policies. Users not complying with these policies could be subject to disciplinary action. Policy awareness and acknowledgment, by signing the acknowledgment form, is required before access will be granted.

### 3.3.2. Authorized Users:

These Users are those who require Internet Access as part of their duty/role and are further Categorized as

- Management
- Administrative Staff
- Faculty
- Clerical Staff
- Students

### 3.3.3. Unauthorized Users:

Users who do not require Internet Access as part of their duty/role. Users not authorized as per the above list, can also avail of the Group Internet Services by paying a Monthly Fee of Rs. 100/-

### 3.3.4. Approval

Internet access is requested by the user by submitting an IT Access Request form approved by Deans/Directors to the concerned IT department.

### 3.3.5. Removal of Privileges

3.3.5.1. Internet access will be discontinued upon termination of employee, completion of contract, end of service of non-employee, or disciplinary action arising from violation of this policy. In the case of a change in job function and/or transfer the original access code will be discontinued, and only reissued if necessary and a new request for access is approved.

3.3.5.2. Internet access for students shall be discontinued upon completion of course/ transfer/migration etc.

3.3.5.3. All user IDs that have been inactive for thirty (30) days will be revoked. The privileges granted to users must be reevaluated by management annually. In response to feedback from management, systems administrators must promptly revoke all privileges no longer needed by users.

3.3.5.4. The Group also prohibits the conduct of a political activity, engaging in any form of intelligence collection, engaging in fraudulent activities, or knowingly disseminating false information

3.3.5.5. Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law

- 3.3.5.6. Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- 3.3.5.7. Any form of gambling.
- 3.3.5.8. Unauthorized downloading of any shareware programs or files for use without authorization in advance from the IT Department and the user's manager.
- 3.3.5.9. Playing of any games. Forwarding of chain letters. Participation in any on-line contest or promotion etc

**3.4. Internet Access Request Form**

Applicant's Name:	<input type="text"/>
Mobile No:	<input type="text"/>

<b>For Students</b>			
University Roll No	<input type="text"/>	Name of course currently enrolled:	<input type="text"/>
Enrollment No	<input type="text"/>	Batch	<input type="text"/>

<b>For Employees</b>					
Designation	<input type="text"/>	School/Department	<input type="text"/>		
Employee Cat:	<input type="checkbox"/> Management	<input type="checkbox"/> Administrative Staff	<input type="checkbox"/> Faculty	<input type="checkbox"/> Clerical Staff	<input type="checkbox"/> Student
EID No:	<input type="text"/>				

<b>Services Required</b>	<input type="checkbox"/> Email	<input type="checkbox"/> Internet Paid	<input type="checkbox"/> Internet Unpaid
--------------------------	--------------------------------	--	--

**Terms and Conditions**

1. By signing below, the individual requesting Internet access through company computing resources hereby acknowledges receipt of and compliance with the Internet Usage Policy.
2. Furthermore, the undersigned also acknowledges that he/she has read and understands the Internet / Email and Communication policy before signing this form.
3. Internet access will not be granted until this acknowledgment form is signed by the individual's Dean/Director
4. After completion, the form is filed in file maintained by the IT department separately for employees and students. These acknowledgment forms are subject to internal audit.
5. Wifi Users are requested to install antivirus software and update them regularly.
6. User's password will gets disabled when not used for 60 days and the account will be deleted after 6 months.
7. Rayat and Bahra University does not share any user information with anyone unless authorized by the competent authority of the University.
8. The Wi-Fi enablement under the password is exclusive to you. You will be solely responsible for its use and wrong use.
9. It is informed that any action or communication, spoken or in writing or by photo images done through internet, whether by email or by Wi-Fi will be attributed to you even if it has been done using your password unauthorized or with your consent.
10. You should always understand that it would be presumed that you are aware of the legal consequences of any wrong use of internet etc.
11. All actions on internet are punishable in the same manner as if done in the physical space.
12. I undertake that I would keep my password secret for Wi-Fi and I understand that it is my responsibility to maintain its secrecy and I assume full responsibility for the same from the moment the password is given to me.
13. I also understand that if an unauthorized person accesses the email or internet on my password, I will be called to question and would have to own responsibility for the same. I have put my signature onto this application form to acknowledge this accountability/ responsibility.

I have read and understood the terms and conditions and agree to abide by them.



Applicants Signature

Date

Dean/Director

Date

-----

User ID Assigned: _____	<b>FOR OFFICE USE</b>	Temporary Password: _____
File No: _____		Date: _____

-----

### 3.5. Physical Internet Connection

All physical internet connections or connections to other private networks shall be authorized and approved by the campus IT department. Most users will access the internet through the connection provided for their office by the IT department. Any additional connections must be approved by the IT department. These additional connections include but are not limited to:

- a) Direct modem connection from a computer or communication device which may allow a connection to the network.
- b) Data Cards
- c) Any multipurpose printing and FAX machines which have both a phone and network connection must be examined and approved for use by the IT department.
- d) If any computers or other devices have wireless capability, the wireless capability must be turned off before connecting to the network unless it is approved for wireless operation by the IT department when connected to the network.

### 3.6. Internet Control and Logging System

- 3.6.1. A UTM will be operated on the each campus network for Internet control and logging:
- 3.6.2. UTM would have capabilities of creating user categories having different internet usage requirement and allow access accordingly
- 3.6.3. UTM shall have Virus Control enabled.
- 3.6.4. The ability to prevent users from visiting inappropriate, pornographic, or dangerous web sites. It will have its database of categorized websites updated regularly.
- 3.6.5. The ability to log user internet activity including:
  - 1) Time of the internet activity.
  - 2) Duration of the activity.
  - 3) The website visited.
  - 4) Data and type of data downloaded
- 3.6.6. Proxy Server shall be used if necessary, to cache web pages to increase the internet connection speed.

(Annexure IV)

## Anti-virus and Malware policy

### 1. Overview

This policy defines anti-virus and Malware policy on every computer/Server including how often a virus scan is done, how often updates are done, what programs will be used to detect, prevent, and remove malware programs. It defines what types of files attachments are blocked by the mail server. It also specifies whether an anti-spam firewall will be used to provide additional protection. It may also specify how files can enter the trusted network and how these files will be checked for hostile or unwanted content. For example it may specify that files sent to the enterprise from outside the trusted network be scanned for viruses by a specific program.

### 2. Purpose

This policy is designed to protect the organizational resources against intrusion by viruses and other malware.

### 3. Anti-Virus Policy

- a) The Group will use a UTM for perimeter defense which will provide antivirus and spam protection capabilities for traffic entering the Network.
- b) The Group may also use an endpoint anti-virus product for anti-virus protection for each work station/laptop/server. Products recommended are "Quick Heal Total Security"/Symantec.
- c) Microsoft Security shall also be used at endpoint in addition to the antivirus software.
- d) The following minimum requirements shall remain in force.
  1. The anti-virus product shall be operated in real time on all servers and client computers. The product shall be configured for real time protection.
  2. The anti-virus library definitions shall be updated at least once per day.
  3. Full Anti-virus scans shall be done a minimum of once per week on all user controlled workstations/laptops and servers.
- e) Anti-virus definition updates shall be downloaded on a server and all computers shall connect to that server for updating their antivirus library definitions. This is done for optimal usage of internet connection.

- f) When a virus is found or malware is found, the policy shall be to delete the email. If the email is from a known source, the sender shall be notified.
- g) No one should be able to stop anti-virus definition updates and anti-virus scans except for domain administrators.

## Asset Control Policy

### 1. Overview

All employees and personnel that have access to Group computer systems must adhere to the IT asset control policy defined below in order to protect the security of the network, protect data integrity, and protect and control computer systems and organizational assets. The asset control policy will not only enable organizational assets to be tracked concerning their location and who is using them but it will also protect any data being stored on those assets. This asset policy also covers disposal of assets.

IT assets should not be confused with nor tracked with other organizational assets such as furniture. One of the main reasons to track IT assets other than for property control and tracking is for computer security reasons. A separate IT asset tracking policy will enable the organization to take measures to protect data and networking resources.

This policy will define what must be done when a IT asset is moved from one building to another or one location to another. This policy will provide for asset tracking database to be updated so the location of all computer equipment is known. This policy will help network administrators protect the network since they will know what user and computer is at what station in the case of a worm infecting the network.

### 2. Purpose

This policy is designed for asset control of IT Infrastructure for preventing loss of data or organizational assets.

### 3. Assets Tracked

The following Assets shall be tracked.

- a) Desktop workstations
- b) Laptop mobile computers
- c) Printers, Copiers, FAX machines, multifunction machines
- d) Scanners
- e) Servers
- f) Firewalls
- g) Routers
- h) Switches

### 4. Asset Tracking Requirements

- 4.1. All assets must have an ID number. An asset tracking database shall be created to track assets. This asset tracking database shall be maintained by Campus IT Department.
- 4.2. When an asset is acquired, an ID will be assigned for the asset and its information shall be entered in the asset tracking database.
- 4.3. Upon movement of Asset from one location to another, intimation of the same shall be provided to IT Department indicating the new location, date of movement, authorized by.

## **5. Asset Disposal**

- 5.1. When IT assets reach the end of their useful life/ or are to be disposed, they would be sent to the IT Department for proper disposal.
- 5.2. IT Department will securely erase all storage mediums in accordance with current industry best practices.
- 5.3. Equipment which is working, but reached the end of its useful life will be made available for purchase by employees.
- 5.4. Finance and Information Technology will determine an appropriate cost for each item.
- 5.5. All purchases are final. No warranty or support will be provided with any equipment sold.
- 5.6. Any equipment not in working order or remaining from non disposal to employees would be disposed as per disposal policy to be indicated in the Purchase & Store Manual.
- 5.7. Prior to leaving the premises, all equipment shall be removed from the asset tracking database.

## **6. Server Room Control.**

- 6.1. Only Persons authorized by IT Department shall operate in Serer Room.
- 6.2. The key to the Rack in which the Assets are hoisted shall be available with Engineer IT Department with a duplicate key placed under lock & Key at a designated place.
- 6.3. Under no circumstances, the server, UTM and router password shall be given to any other person.

## Mobile Computer Policy

### 1. Overview

This policy defines the use of mobile computers in the organization. It defines:

- a) The process that mobile computers must meet to leave the network. Both the device and any sensitive data should be password protected.
- b) How mobile computers and devices will be protected while outside the organizational network.
- c) The process that mobile computers must meet to enter the corporate network when being brought into a building owned by the organization.

### 2. Purpose

This policy is designed both to protect the confidentiality of any data that may be stored on the mobile computer and to protect the organizational network from being infected by any hostile software when the mobile computer returns. This policy also considers wireless access.

### 3. Scope

This policy covers any computing devices brought into the Group or connected to the Group network using any connection method. This includes but is not limited to desktop computers, laptops, and palm pilots.

### 4. Responsibility

The user of the mobile computer will accept responsibility for taking reasonable safety precautions with the mobile compute. The computer user will not be allowed to have administrative rights unless granted special exception by the network administrator. The user of the computer agrees not to use the mobile computer for personal business.

### 5. Mobile Computer Protection

**5.1.** Any mobile computer owned by the organization shall at all times operate the following for its own protection:

- a) Antivirus program which shall be configured for real time protection, to retrieve updates daily.
- b) Full scan to be done on the Mobile Computer when joining the network

- c) Windows Firewall, with the latest possible updates. The program shall be operational any time the computer is connected to any untrusted network including the internet to protect the computer from worms and other malware.
- d) Additional malware protection software shall be active on the computer in accordance with the anti-virus and malware policy.
- e) It shall be ensured that unauthorized persons cannot gain access to the computer without a proper user identification and password. Operating systems that do not safely support this process shall not be used in mobile computers.
- f) Policy for computers being used for travel - Protection of these computers in addition shall be the encryption of all sensitive data and a requirement for a valid user ID to operate the computer.
- g) If there is a chance that the user will view any sensitive data using their web browser or other program, cached data will need to be encrypted. Cached data that is stored locally such as cached data from the user's browser will be set to be encrypted using the encrypting file system (EFS).



## Email & Communication Policy

### 1. Purpose

The purpose of this policy is to ensure the proper use of Group's email system and make users aware of what Group deems as acceptable and unacceptable use of its email system. The Group reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

### 2. Legal Risks

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of e-mail:

- If you send emails with any defamatory, offensive, racist or obscene remarks, you can be held liable.
- If you forward emails with any defamatory, offensive, racist or obscene remarks, you can be held liable.
- If you send an attachment that contains a virus, you can be held liable.

By following the guidelines in this policy, the email user can minimize the legal risks involved in the use of e-mail. If any user disregards the rules set out in this Email Policy, the user will be fully liable and Group will disassociate itself from the user as far as legally possible.

### 3. Legal requirements

The following rules are required by law and are to be strictly adhered to:

- It is strictly prohibited to send or forward emails containing defamatory, offensive, racist or obscene remarks. If you receive an e-mail of this nature, you must promptly notify your supervisor.
- Do not send unsolicited email messages.
- Do not forge or attempt to forge email messages.
- Do not send email messages using another person's email account.
- Do not copy a message or attachment belonging to another user without permission of the originator.
- Do not disguise or attempt to disguise your identity when sending mail.

### 4. Best practices

Group considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image

and delivering good customer service. Therefore Group wishes users to adhere to the following guidelines:

#### 6.4. Writing emails:

- Write well-structured emails and use short, descriptive subjects.
- Group's email style is informal. This means that sentences can be short and to the point. You can start your e-mail with 'Hi', or 'Dear', and the name of the person. Messages can be ended with 'Best Regards'. The use of Internet abbreviations and characters such as smileys however, is not encouraged.
- Signatures must include your name, job title and Group name. A disclaimer will be added underneath your signature (see Disclaimer)
- Use the spell checker before you send out an email.
- Do not send unnecessary attachments. Compress attachments larger than 200K before sending them.
- Do not write emails in capitals.
- Do not use cc: or bcc: fields unless the cc: or bcc: knows what action, if any, to take.
- If you forward mails, state clearly what action you expect the recipient to take.
- Only mark emails as important if they really are important.
- Only use Group Email.
- Use of Other Emails for official Purposes (Gmail, Yahoo etc) should be avoided.

#### 6.5. Replying to emails:

- Emails should be answered within at least 8 working hours, but users must endeavor to answer priority emails within 4 hours.
- Priority emails are emails from existing customers/students and business partners.

#### 6.6. Maintenance:

- Delete any email messages that you do not need to have a copy of, and set your email client to automatically empty your 'deleted items' on closing.

#### 6.7. Personal Use

Although Group's email system is meant for business use, Group allows the reasonable use of email for personal use if certain guidelines are adhered to:

- Personal use of email should not interfere with work.
- Personal emails must also adhere to the guidelines in this policy.
- Personal emails are kept in a separate folder, named 'Private'. The emails in this folder must be deleted weekly so as not to clog up the system.
- The forwarding of chain letters, junk mail, jokes and executables is strictly forbidden.
- On average, users are not allowed to send more than 2 personal emails a day.
- Do not send mass mailings.

- All messages distributed via the Group's email system, even personal emails, are Group's property.

#### 6.8. Confidential information

Avoid sending confidential information by e-mail. If you do, you must secure the information by including it in a Microsoft Word or Excel file and protecting it with a password. Then provide the recipient with the password by means of other communication, for instance by telephone.

#### 6.9. Disclaimer

The following disclaimer will be added to each outgoing email:

'This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the Group. Finally, the recipient should check this email and any attachments for the presence of viruses. The Group accepts no liability for any damage caused by any virus transmitted by this email.'

#### 6.10. System Monitoring





You must have no expectation of privacy in anything you create, store, send or receive on the Group's computer system. Your emails can be monitored without prior notification if [Group] deems this necessary. If there is evidence that you are not adhering to the guidelines set out in this policy, the [Group] reserves the right to take disciplinary action, including termination and/or legal action.































#### 6.11. Email accounts






















All email accounts maintained on our email systems are property of [Group]. Passwords should not be given to other people and should be changed once a month. Email accounts not used for 60 days will be deactivated and possibly deleted.

#### 6.12. Blocked Attachment Types

Following attachments will be blocked generally for emails. This is because these attachment types are dangerous containing active content which may be used to infect a computer with hostile software or because these attachment types are commonly successfully used by virus programs or malware to spread.

 <a href="#">file extension ade</a>	Microsoft Access compiled project file
 <a href="#">file extension app</a>	Executable application file
 <a href="#">file extension bas</a>	Basic source code
 <a href="#">file extension bat</a>	Batch file (executable)

 <a href="#">file extension cer</a>	Internet security certificate
 <a href="#">file extension chm</a>	Microsoft compiled HTML help file
 <a href="#">file extension cmd</a>	Windows NT command script file
 <a href="#">file extension com</a>	DOS CP/M command file
 <a href="#">file extension com</a>	Command executable file
 <a href="#">file extension cpl</a>	Microsoft Windows Control Panel extension
 <a href="#">file extension crt</a>	Internet security certificate (GlobalSign certificate file)
 <a href="#">file extension csh</a>	Unix shell script
 <a href="#">file extension csh</a>	csh script file
 <a href="#">file extension exe</a>	Executable file
 <a href="#">file extension fpx</a>	Visual FoxPro compiled program
<a href="#">file extension gadget</a>	Windows sidebar gadget file
 <a href="#">file extension hlp</a>	Microsoft help file
 <a href="#">file extension hta</a>	HTML program
 <a href="#">file extension inf</a>	Windows installation script
 <a href="#">file extension ins</a>	Microsoft IIS Internet communications settings file
 <a href="#">file extension ins</a>	Microsoft Windows Internet Naming Service file
 <a href="#">file extension isp</a>	Internet Service Provider settings (Internet Explorer) file
 <a href="#">file extension js</a>	JavaScript file
 <a href="#">file extension jse</a>	JScript encoded script file
 <a href="#">file extension ksh</a>	Unix shell script
 <a href="#">file extension lnk</a>	Windows Shortcut
<a href="#">file extension mad</a>	Microsoft Access module shortcut file
<a href="#">file extension mas</a>	Microsoft Access stored procedures file
<a href="#">file extension mav</a>	Microsoft Access view file
<a href="#">file extension maw</a>	Microsoft Access data access page file
<a href="#">file extension mda</a>	Microsoft Access 2 workgroup file
<a href="#">file extension mda</a>	Microsoft Access add-in file
<a href="#">file extension mdb</a>	Microsoft Access database file
<a href="#">file extension mde</a>	Microsoft Access compiled database (application) file
<a href="#">file extension mdt</a>	Microsoft Access database template file
<a href="#">file extension mdz</a>	Microsoft Access wizard template file
 <a href="#">file extension mobileconfig</a>	Apple iPhone mobile configuration profile
 <a href="#">file extension msc</a>	Microsoft management console control file
<a href="#">file extension msi</a>	Microsoft Windows Installer installation package file
 <a href="#">file extension msp</a>	Windows Installer patch file
 <a href="#">file extension mst</a>	Microsoft Windows SDK setup script
 <a href="#">file extension mst</a>	Windows Installer Transform
 <a href="#">file extension ops</a>	Microsoft Office profile settings file
<a href="#">file extension pcd</a>	Microsoft Visual Test file
 <a href="#">file extension pif</a>	Microsoft Windows Program Information File (PIF)
 <a href="#">file extension prf</a>	Microsoft Windows system file
 <a href="#">file extension prf</a>	Microsoft Profiler output

 <a href="#">file extension prg</a>	Program file
 <a href="#">file extension prg</a>	Program source file
 <a href="#">file extension pst</a>	Microsoft Exchange address book file
 <a href="#">file extension reg</a>	Registry data file for Windows
 <a href="#">file extension scf</a>	Windows Explorer shell command file
 <a href="#">file extension scr</a>	Microsoft Windows screensaver file
 <a href="#">file extension sct</a>	Microsoft Windows script component file
 <a href="#">file extension sct</a>	FoxPro additional (FPT) screen description file
 <a href="#">file extension shb</a>	Microsoft Windows shortcut into a document
 <a href="#">file extension shs</a>	Microsoft Windows Shell Scrap Object file
 <a href="#">file extension tmp</a>	Temporary file
 <a href="#">file extension url</a>	Internet Shortcut - URL - Uniform Resource Locator
 <a href="#">file extension vbe</a>	Microsoft Visual Basic script file
 <a href="#">file extension vbs</a>	Visual Basic for applications script file
 <a href="#">file extension vss</a>	Microsoft Visio smartshapes file
 <a href="#">file extension vst</a>	Microsoft Visio flowchart file
 <a href="#">file extension vsw</a>	Microsoft Visio workspace file
 <a href="#">file extension ws</a>	Microsoft Windows script file
 <a href="#">file extension wsc</a>	Microsoft Windows scripting component file
 <a href="#">file extension wsf</a>	Microsoft Windows scripting file
 <a href="#">file extension wsh</a>	Microsoft Windows Scripting Host file
file extension zip/rar	ZIP/RAR Files

The above list shall be updated from time to time.

When an email breaks the rules and contains an illegal file attachment the following action is recommended.

Remove the attachment and let the email go through. - This would let the receiver know that someone tried to send them an illegal attachment. If the attempt was a legitimate one, they could contact the sender and tell them what to do to get the attachment sent.

**Annexure VIII****Backup Policy Guidelines****1. Overview**

This policy defines the backup policy guidelines for computers within the organization which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers.

**2. Purpose**

This policy is designed to protect data in the organization to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

**3. Scope**

**3.1.** All users are responsible for arranging adequate data backup procedures for the data held on IT systems assigned to them.

**3.2.** The disaster recovery procedures in this policy apply to all LAN Administrator, System Administrators, and Application Administrators who are responsible for systems or for a collection of data held either remotely on a server or on the hard disk of a computer.

**4. Definitions**

- a) Backup - The saving of files onto tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
- b) Archive - The saving of old or unused files onto tape or other offline mass storage media for the purpose of releasing on-line storage room.
- c) Restore - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

**5. Backups****5.1. Desktop**

- All Files in Libraries, Personal Folders, Folder of Outlook Express Database and System Image, Any other essential Directory to be backed up using Backup and Restore Features of OS.
- Backup Registry Files
- At least three generations of back-up data must be retained at any one time (grandfather/father/son).
- Backup Drive Partioned Drive on the Hard Disk, CD,DVD. If Backup is taken on CD/DVD, the same may be got issued from IT Department/ Security & IT Engineers , labeled and returned to the IT Department/ Security & IT Engineers for safe custody.

**5.2. Data Base Server Backup**

- Database Transactions shall be backed up using full recovery model using full, differential and transaction-log backups.
- Full recovery model offers the most robust recovery plan. Under this model all transactions including bulk-logged operations, are fully logged in the transaction log. Even system functions such as index creation are o logged. The primary benefit of this model is

that every committed transaction in the database can be restored right up to the point when failure occurred.

- Full Database shall be backed up Once a Week (Monday)
- Differential backup of Database shall be taken up every day(Tuesday to Saturday)
- The transaction log is backed up throughout the day, every three hours.
- IT dept shall create the maintenance schedule & the job for backup based upon the above guidelines. The job shall be executed automatically by SQLServerAgent at the scheduled time .
- The backup files shall be copied once a day and kept in the safe place.
- Periodic exercise shall be undertaken to restore the data to check the integrity of the backup files.

### 5.3. Windows Server 2008

- The Windows Server Backup feature in Windows Server 2008 to be used for day-to-day backup and recovery using the built in Wizards for running backups and recoveries.
- The features can be used to back up a full server (all volumes), selected volumes, or the system state.
- It is possible to recover volumes, folders, files, certain applications, and the system state. And, in case of disasters like hard disk failures, one can perform a system recovery, which will restore the complete system onto the new hard disk, by using a full server backup and the Windows Recovery Environment.
- Windows Server Backup can be used to create and manage backups for the local computer or a remote computer.
- Backups can be scheduled to run automatically.

## 6. Backup Responsibility

- The responsibility for backing up data held on the workstations/laptops falls entirely to the User
- Campus IT Department shall be responsible for taking the Application, Database & Windows Server backup.

## 7. Storage of backup media

Backup media must, at all times, be stored in one of the following areas:

- a) Data Closet
- b) A single office room that is locked when unattended
- c) Inside locked furniture within Group Internal Space
- d) An approved off-site media storage facility

## Annexure IX

**Information Sensitivity Policy****1. Purpose**

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Group without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect Group Confidential information (e.g., Group Confidential information should not be left unattended in conference rooms).

**2. Policy****2.1. Group Public**

Group Public information is information that has been declared public and can freely be given to anyone without any possible damage to Group.

**2.2. Group Confidential**

Group Confidential contains all other information. Included is information like trade secrets, designs, development programs, sales leads , vendor purchase pricing , telephone directories, and other information integral to the success of our Group.

Confidential is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner.

A subset of Group Confidential information is "Group Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to Group by that Group under non-disclosure agreements and other contracts.

***The Details of which information is Public & which is Confidential shall be worked out by P&A Department and circulated to employees along with access, distribution , Storage & Disposal control for the information in hardcopy or electronic form.***



## Removable Media Policy

### 1. Overview

Removable media has been directly tied to the loss of sensitive information in many organizations. To ensure controlled use of removable media devices to store and transfer information by users who have access to information, information systems and IT equipment for the purposes of conducting official business.

### 2. Purpose

The policy establishes the principles and working practices that are to be adopted by all users in order for data to be safely stored and transferred on removable media.

This policy aims to ensure that the use of removable media devices is controlled in order to:

- ✓ Enable the correct data to be made available where it is required.
- ✓ Maintain the integrity of the data.
- ✓ Prevent unintended or deliberate consequences to the stability of Computer Computer network.
- ✓ Avoid contravention of any legislation, policies or good practice requirements.
- ✓ Build confidence and trust in the data that is being shared between systems.
- ✓ Maintain high standards of care in ensuring the security of Protected and Restricted information.
- ✓ Prohibit the disclosure of information as may be necessary by law.

### 3. Scope

This policy applies to all Employees of the Group, contractual third parties etc. who have access to Group information, information systems or IT equipment and intends to store any information on removable media devices.

### 4. Definition

This policy should be adhered to at all times, but specifically whenever any user intends to store any information used by the Council to conduct official business on removable media devices.

Removable media devices include, but are not restricted to the following [amend list as appropriate]:

- CDs.
- DVDs.

- Optical Disks.
- External Hard Drives.
- USB Memory Sticks (also known as pen drives or flash drives).
- Media Card Readers.
- Digital Cameras.

## 5. Risks

This policy aims to mitigate the following risks [amend list as appropriate]:

- Disclosure of Group Confidential information as a consequence of loss, theft or careless use of removable media devices.
- Contamination of Group network or computers through the introduction of viruses through the transfer of data from one form of IT equipment to another.
- Group reputational damage as a result of information loss or misuse.

## 6. Policy

### 6.1. Restricted Access to Removable Media

It is Group policy to prohibit the use of all removable media devices. The use of removable media devices will only be approved if a valid business case for its use is developed. There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

Requests for access to, and use of, removable media devices must be made to IT Department. Approval for their use must be given by Concerned IT Department.

**6.2.** All removable media devices and any associated equipment and software must only be purchased and installed by IT Department.

**6.3.** Non-Group removable media devices must not be used to store any information used to conduct official business, and must not be used with any Group owned or leased IT equipment.

### 6.4. Security of Data

Copies of any data stored on removable media must also remain on the source system or networked computer until the data is successfully transferred to another networked computer or system.

In order to minimize physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.

Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whilst in their care or under their control.

All data stored on removable media devices must, where possible, be encrypted. If this is not possible, then all Group Confidential data held must be encrypted.

#### **6.5. Incident Management**

It is the duty of all users to immediately report any actual or suspected breaches in information security to

#### **6.6. Third Party Access to Group Information**

No third party (external contractors, partners, agents, the public or non-employee parties) may receive data or extract information from the Group network, information stores or IT equipment without explicit agreement/approval.

#### **6.7. Preventing Information Security Incidents**

Damaged or faulty removable media devices must not be used. It is the duty of all users to contact IT Department should removable media be damaged.

Virus and malware checking software approved by the Group must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded. The data must be scanned by virus checking software products, before the media is loaded on to the receiving machine

While in transit or storage the data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity. Encryption or password control must be applied to the data files unless there is no risk to the Group, other organizations or individuals from the data being lost whilst in transit or storage.

#### **6.8. Disposing of Removable Media Devices**

Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage. Any previous contents of any reusable media. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools. All removable media devices that are no longer required, or have become damaged, must be returned to IT Department.

#### **6.9. User Responsibility**

All considerations of this policy must be adhered to at all times when using all types of removable media devices. However, special attention must be paid to the following when using USB memory sticks (also known as pen drives or flash drives), recordable CDs, DVDs and diskettes:

- Any removable media device used in connection with Group equipment or the network or to hold information used to conduct official Group business must only be purchased and installed by [Name an appropriate department – e.g. IT Services]. Any removable media device that has not been supplied by IT must not be used.
- All data stored on removable media devices must be encrypted where possible.
- Virus and malware checking software must be used when the removable media device is connected to a machine.
- Only data that is authorised and necessary to be transferred should be saved on to the removable media device. Data that has been deleted can still be retrieved.
- Removable media devices must not to be used for archiving or storing records as an alternative to other storage equipment.
- Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.