RYLANDS HIGH SCHOOL HIGH SCHOOL

SCHOOLS NETWORK
Information and Communication Technology
Acceptable Use Policy

Contents

1. GUIDELINE PURPOSE

The purpose of this guideline is to ensure the proper use of Information Communication and Technology (ICT) assets of the SCHOOLS NETWORK. The guideline applies to any ICT asset the SCHOOLS NETWORK has or may install in the future. Users have a responsibility to use ICT assets in an efficient, effective, ethical and lawful manner.

2. SCOPE OF APPLICATION

This guideline is applicable to all RYLANDS HIGH SCHOOL employees, school learners, contractors and agents who act on behalf of RYLANDS HIGH SCHOOL or are in its employment and are end users of the RYLANDS HIGH SCHOOL IT Systems, equipment and Infrastructure.

3. GUIDING PRINCIPLES

The primary purpose of the Acceptable Use Guideline is to protect the SCHOOLS NETWORK, officials, school learners, contractors, other spheres of government and other parties from illegal or damaging actions by individuals, whether deliberate or unintended. The primary guiding principle is that SCHOOLS NETWORK information technology assets should mainly be used for Education business purposes.

This Policy is subject to change as the need arises.

4. LEGAL FRAMEWORK

This guideline draws its mandate from the following prescripts:

- The Electronic Communications and Transactions Act (Act No. 25 of 2002)
- The Public Service Act (Act No. 111 of 1984)
- The National Strategic Intelligence Act (Act No. 39 of 1994)
- The Protection of Information Act (Act No. 84 of 1982)
- The National Archives and Record Service of South Africa Act (Act No. 43 of 1996)
- ABS/ISO 27k
- The Minimum Information Security Standards (MISS) and/or the Guidelines for the handling of Classified Information (SP/2/8/1)
- The Regulation of Interception of Communications and Provision of Communication-related Information Act 2002 (Act No. 70 of 2002).
- South African Schools Act No 84 of 1996 with Amendments up to 2011

5. GUIDELINE STATEMENT

5.1. General Provisions

5.1.1 The SCHOOLS NETWORK is governed by a broad range of legislation regulating telecommunications including, but not limited to, the Electronic Communications and Transactions Act, 2002, and the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, (the Interception Act).

5.1.2 Users are bound by all relevant legislation and policies regulating telecommunications and electronic communications and undertake at all times to act in accordance with all relevant legislation and policies. Users acknowledge that they have been granted access by the organization to telecommunications information technology and resources, including e-mail and Internet access. The sole reason for providing such access to Users is to perform duties and responsibilities in accordance with their job function or other official purposes of the SCHOOLS NETWORK.

5.1.3 Users acknowledge that they have no expectation of privacy when utilizing any telecommunications equipment and resources operated under the auspices of the SCHOOLS NETWORK and they grant permission to the SCHOOLS NETWORK to intercept, monitor, read, filter, block or otherwise act upon any electronic telecommunication, stored file or indirect communication which is or has been under their control, received by them or transmitted by them as contemplated in the RICA Act.

5.2. Use of SCHOOLS NETWORK IT Equipment

5.2.1 The end user shall be responsible for his or her workstation or portable computer.

5.2.2 If the equipment is stolen, damaged, borrowed or otherwise unavailable for normal business activities it shall immediately be reported to the IT Helpdesk at 021 900 7123.

5.2.3 SCHOOLS NETWORK equipment must not be removed from SCHOOLS NETWORK premises without a valid removal permit.

5.2.4 Equipment must be physically secured or physically protected to guard against theft.

5.2.5 Users must ensure that equipment assigned to them has been added to the asset inventory and has received a unique identifier and classified in accordance with the Asset register.

5.2.6 Users with SCHOOLS NETWORK equipment at their homes shall safeguard the equipment as required by *IT Security Policies*.

Users shall ensure that they keep mobile equipment in their possession at all times when they are in a public place.

5.3. Desktop Computer Use

5.3.1. The device (Computer Desktop, Laptop) may not be connected to two or more networks simultaneously.

5.3.2. Users must be supplied with a username and password in order to access services on the school's network of the SCHOOLS NETWORK.

5.3.3. Users must keep passwords secure and not share their account credentials. Users are responsible for the security of their passwords and accounts.

5.3.4. The device must be locked or logged off when unattended.

5.3.5. The device must be kept up to date with the latest anti-virus software and virus definitions and Operating System updates.

5.3.6. The user must not disable, and/or change the configuration of the anti-virus software.

5.3.7. Users shall not load any illegal or unapproved software onto RYLANDS HIGH SCHOOL equipment

5.3.8. Users acknowledge sole responsibility for any unauthorized or pirated software found in their possession or on the systems and equipment allocated to or used by them.

5.4. Email

The SCHOOLS NETWORK supports the installation and usage only of approved email clients.

Usernames will be assigned by the SCHOOLS NETWORK and reflect internally mandated e-mail naming conventions.

5.4.1. Acceptable Email Use

5.4.1.1. Communicating in a professional manner.

5.4.1.2. Personal communications that are brief and do not interfere with work responsibilities.

5.4.1.3. Electronic messages are frequently inadequate in conveying mood and context. Users should carefully consider how the recipient might interpret a message before composing or sending the message.

5.4.2. Unacceptable Use of Email

5.4.2.1. Creating and exchanging messages that can be interpreted as offensive, harassing, obscene, racist, sexist, ageist, pornographic or threatening.

5.4.2.2. Creating and exchanging information that is in violation of copyright or any other law. The SCHOOLS NETWORK is not responsible for use of e-mail that contravenes the law.

5.4.2.3. Opening file attachments from an untrustworthy source or with a suspicious or unexpected subject line.

5.4.2.4. Sending confidential information to unauthorized people or violating the Minimum Information Security Standards. Otherwise using e-mail in a way that increases the SCHOOLS NETWORK's legal and regulatory liability.

5.4.2.5. Communications that strain the SCHOOLS NETWORK or other systems unduly, such as sending large files to large distribution lists.

5.4.2.6. Circulating chain letters and/or commercial offerings.

5.4.2.7. Circulating unprotected data and personally identifiable client/citizen data that would violate section 14 of the Constitution.

5.4.2.8. Promoting or publishing a User's political or religious views, operating a business or for any undertaking that offers personal gain.

5.4.2.9. Using the e-mail system for any purpose or in any manner that may prejudice the rights or interests of the SCHOOLS NETWORK or government in any other sphere.

5.5. Internet

Internet usage is granted for the sole purpose of supporting SCHOOLS NETWORK activities. All Internet based transactions originating from within the SCHOOLS NETWORK, are carefully monitored for auditing and compliance purposes.

5.5.1. Acceptable Uses of Internet

5.5.1.1 Accessing web-based applications and tools.

5.5.1.2 Communication between Officials and non-Officials for business purposes.

5.5.1.3 Review of possible vendor web sites for product information or educational purposes.

5.5.1.4 Reference regulatory or technical information in line with the relevant the job description or official functions.

5.5.1.5 Accessing of Government web sites and portals.

5.5.1.6 Conducting research in line with relevant job description or official functions.

5.5.2. Unacceptable Uses of Internet

Acquisition, storage, and dissemination of data that are illegal, pornographic, or which negatively depict race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language and birth is specifically prohibited.

The SCHOOLS NETWORK also prohibits engaging in fraudulent activities, or knowingly disseminating defamatory materials.

Other activities that are strictly prohibited include, but are not limited to:

5.5.2.1. Accessing information that is not within the scope of the user's work. This includes unauthorized accessing and / or reading of SCHOOLS NETWORK information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.

5.5.2.2. Deliberate pointing or hyper-linking of the SCHOOLS NETWORK's Web sites to other Internet sites whose content may be inconsistent with or in violation of the aims or policies of the SCHOOLS NETWORK.

5.5.2.3. Any conduct that would constitute or encourage a criminal offence, lead to civil liability, or otherwise violates any regulations, directives or the common law.

5.5.2.4. The use, transmission, duplication, or voluntary receipt of material that infringes on the copyright, trademarks, trade secrets, or patent rights of any person or organization. [Officials must accept that all materials on the Internet are copyrighted and/or patented unless specific notices expressly state otherwise].

5.5.2.5. Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls and the express permission from the relevant mandated parties.

5.5.2.6. Any form of on-line gambling and gaming.

5.5.2.7. Using the internet for any purpose or in any manner that may prejudice the rights or interests of the SCHOOLS NETWORK or RYLANDS HIGH SCHOOL in any other sphere.

5.6. Information Security

.

5.6.1 All users accessing SCHOOLS NETWORK information shall preserve the confidentiality, integrity and availability of information.

5.6.2 Users must ensure that all media, such as memory sticks, drives and CDs, to be discarded is formatted and cleansed of all data. If media is damaged and cannot be formatted the media shall be destroyed in such a manner that repair of the media is impossible.

5.6.3 Users must ensure that all media used for the storage of data is stored in a secure environment and within safe distance of any electromagnetic interference, such as cell phones, that can damage the media.

5.6.4 Users must not share folders to all on the network from their computers without proper user logon authentication access security in place.

5.6.5 Users must not make any unauthorized copies of or modifications to the contents of any SCHOOLS NETWORK information resources.

5.6.6 Users must handle all information resources in a secure manner.

5.6.7 Users must ensure that information under their control is backed up in line with the criticality of the information to SCHOOLS NETWORK.

6 PRIVACY GUIDELINES

6.1 The SCHOOLS NETWORK maintains the right to monitor and review e-mail and Internet activity to ensure compliance with this guideline, as well as to fulfilling the SCHOOLS NETWORK's responsibilities in terms of legislation. Users have no expectation of privacy.

6.2 On termination or separation from the SCHOOLS NETWORK, access will be denied to e-mail and SCHOOLS NETWORK Internet, including the ability to download, forward, print or retrieve any message stored in the system, regardless of sender or recipient.

6.3 Officials and learners who leave the SCHOOLS NETWORK will have their mailbox disabled immediately after exiting the organization.

6.4 The SCHOOLS NETWORK reserves the right to intercept, monitor, review and/or disclose any and all messages composed, sent or received. Intercepting, monitoring and reviewing of messages may be performed with the assistance of content filtering software, or by designated SCHOOLS NETWORK Officials.

6.5 The SCHOOLS NETWORK reserves the right to alter, re-route or block the delivery of e-mail messages as appropriate. This includes but is not limited to:

6.5.1 Rejecting, quarantining or removing attachments and/or malicious code from messages that may pose a threat to SCHOOLS NETWORK resources.

6.5.2 Discarding attachments, such as music, that are considered to be of little value and involve a significant resource cost.

6.5.3 Rejecting or quarantining messages with suspicious content.

6.5.4 Rejecting or quarantining messages containing offensive language.

6.5.5 Re-routing messages with suspicious content to designated SCHOOLS NETWORK employees for manual review.

6.5.6 Appending legal disclaimers to messages.

6.6 Electronic messages are permissible as evidence in a court of law.

6.7 Any content created with the e-mail system is considered the intellectual property of the SCHOOLS NETWORK.

7 CYBERBULLYING

7.1 Cyberbullying is the process of using the Internet or mobile devices to send and post any text or images intended to hurt, torment, threaten, embarrass another person and includes any such conduct by way of email, mobile phone and text messages, instant messaging, personal websites and/or chat rooms.

7.2 Cyberbullying takes various forms including –

7.2.1 Instant Messaging (IM)/Text Messaging Harassment: sending hateful or threatening messages to the target/s.

7.2.2 Warning wars: reporting of provoked violations of Internet service providers' terms/website terms which can result in the target being banned from a particular website or social network.

7.2.3 Text wars or text attacks: ganging up on the target, including sending multiple text-messages to the victim's cell phone/email.

7.2.4 Stealing passwords: masquerading as such a person and then posting inappropriate/harmful/illegal posts via such fake profile.

7.2.5 Sending/posting degrading pictures or videos

7.2.6 Outing: sharing someone's secrets or embarrassing information online

7.2.7 Trickery: tricking the target into revealing secrets or embarrassing information and then sharing it online

7.2.8 Excluding: intentionally and maliciously excluding someone from an online or mobile device broadcast group.

7.2.9 Threatening the target with personal violence (including death threats) which may inspire fear or a belief in the victim that such personal violence is to take place.

7.2.10 Cyberstalking: reported and intense harassment, denigration and threats.

7.2.11 Internet Polling/Rating: Who's Hot? Who's Not? Who is the biggest nerd in the sixth grade? These types of questions run rampant on the Internet polls, all created by young people/children.

7.2.12 Posting real or doctored images of the target.

7.2.13 Sharing personal or intimate information about the target;

7.2.14 Sharing contact information about the target coupled with a lewd solicitation ("for a good time call …" or "I am interested in [fill in the blank] …")

7.2.15 Sending Porn and Other Junk E-Mail and IMs: Often cyberbullies will sign their victims up for e-mailing and IM marketing lists, especially to porn sites, resulting in the victim receiving multiple e-mails from porn sites.

7.3 **Role of RYLANDS HIGH SCHOOL**

7.3.1 RYLANDS HIGH SCHOOL strives to create a climate in which every learner can develop academically, socially, spiritually and emotionally. In order for this to happen, Learners need to feel safe and supported, which includes RYLANDS HIGH SCHOOL dealing with all elements of cyberbullying.

7.3.2 To further such principles, RYLANDS HIGH SCHOOL has the right to deal with any incident of cyberbullying when it occurs via the ICT Systems or Personal Devices when linked to the school Wi-Fi.

7.3.3 RYLANDS HIGH SCHOOL is entitled to deal with any incident of cyberbullying where:

7.3.3.1 Cyberbullying takes place off campus or not via the ICT System where the cyberbully/perpetrator is harming/negatively affecting the target's education/schooling or is disrupting learning in the classroom. For example: a learner cannot concentrate at school, is increasingly absent from school or results in fights at school/in the classroom;

7.3.3.2 It impacts on the reputation or integrity of RYLANDS HIGH SCHOOL; an employee, learner or parent

7.3.3.3 A learner confides in a teacher/another learner about cyberbullying off campus or not via the ICT System and the teacher/other learner is concerned that such cyberbullying is harming the learner.

8 SOCIAL MEDIA

8.1 Social Media are the platforms that allow for interactive participation by users to create content and comment (one to one, one to many and many to many). Such communications can take place via any number of devices, such as computers, tables, smartphones etc. Examples include Facebook, Twitter, Instagram, Mxit, Google+, Tumblr, Snapchat etc.

8.2 Some examples:

8.2.1 Blogs - Short for "web-logs", these are sites that can function as on-going journals with multiple entries. Online forums allow members to hold conversations by posting messages. Typically, entries are categorized with "tags" for easy searching. Most blogs allow for reader comments. Examples: Blogger, WordPress, Type Pad.

8.2.2 Micro-blogs - These blogs allow for shorter content posts, typically with a limited set of typed characters allowed. Micro-blogs can be used for status updates and to communicate information to "friends" or "followers" quickly. These are pushed out to anyone subscribed to receive the updates. Examples: Twitter, Tumblr.

8.2.3 Content communities / Media sharing – Services that allow you to upload and share various media, such as pictures and video. For example: YouTube, Flickr.

8.2.4 Bookmarking sites – Services that allow you to save, organize and manage links to various websites and resources around the internet. Example: Delicious, Stumble Upon, Pinterest.

8.3 Rules for Using Social Media

8.3.1 Access to Social Media is a privilege and not a right and is permitted at the sole discretion of RYLANDS HIGH SCHOOL for learners over the age of 13.

8.3.2 RYLANDS HIGH SCHOOL encourages the use of social networking/media (Twitter, Facebook, etc.) as a way to connect with others, share educational resources, create and curate educational content, and enhance the classroom experience. While social networking is fun and valuable, there are some risks you should keep in mind when using these tools. In the social media world, the lines are blurred between what is public or private, personal or professional.

8.3.3 Use good judgment.

8.3.4 Regardless of privacy settings, assume that all of the information you have shared on your social network is public information.

8.3.5 Always treat others in a respectful, positive and considerate manner.

8.3.6 Be responsible and ethical.

8.3.7 Unless you are specifically authorized to represent RYLANDS HIGH SCHOOL as a spokesperson, state that the views expressed in your postings, etc. are your own.

8.3.8 Do not publish, post or release information that is considered confidential or private. If it seems confidential, it probably is. Online "conversations" are never private.

8.3.9 Do not disclose your birth date, address, cellphone number on any public website.

8.3.10 To ensure your safety, be careful about the type and amount of personal information you provide. Avoid talking about personal schedules, situations, your school and places of after school activities.

8.3.11 NEVER give out or transmit personal information of learners, teachers, parents,

8.3.12 Do no post pictures/videos/information of any school activities without the consent of RYLANDS HIGH SCHOOL.

8.3.13 Do not post pictures/videos/information of any learner, parent, teacher, visitor to the school without his/her express written consent.

8.3.14 When using social networking sites, comply with their terms and conditions.

8.3.15 Do not post defamatory or malicious comments about RYLANDS HIGH SCHOOL, any learner, parent, teacher or other employee of RYLANDS HIGH SCHOOL on any social media platform or via any mobile messaging application;

8.3.16 Do not use RYLANDS HIGH SCHOOL name or logos for endorsements.

8.3.17 Do not use the RYLANDS HIGH SCHOOL logo or any school images or iconography on personal social media sites.

8.3.18. Do not use the RYLANDS HIGH SCHOOL name or logo to promote any cause without prior consent.

9 PERSONAL DEVICES

9.1 The use of personal devices is allowed for educational purposes as part of the BYOD initiative.

9.2 RYLANDS HIGH SCHOOL cannot guarantee that a personal device will link to the RYLANDS HIGH SCHOOL Wi-Fi and further that the Wi-Fi will always be available.

9.3 RYLANDS HIGH SCHOOL may limit the number of personal devices on the RYLANDS HIGH SCHOOL Wi-Fi from time to time. Bandwidth use is to be limited and may be restricted.

9.4 Personal Devices –

9.4.1 May only be used during school time, school excursions, and extracurricular activities as long as such use complies with this guideline and any school specific rules

9.4.2 Must be brought to school fully charged. RYLANDS HIGH SCHOOL will at its discretion supply cabling and power points. No learner may unplug any plugs to charge personal devices

9.4.3 Must be switched off if instructed by the educator or set to silent during classroom lessons and all other school activities, such as assemblies, prayers etc. This includes not making or responding to calls, sending or responding to messages (SMS, what's app etc.), playing games, surfing the Internet, accessing any social networking sites

9.4.4 May not be used during tests, assessments and exams

9.4.5 may not be used to take photos or videos in class rooms (other than with the express permission of the teacher), on campus, in change rooms, toilets or in any situation that may harm, cause embarrassment or defame a learner, school, staff, visitors to the RYLANDS HIGH SCHOOL or parents/guardians

9.4.6 Must be clearly marked with the learner's name. Each learner is responsible for the security and insurance of his/her personal devices. RYLANDS HIGH SCHOOL is not responsible for any damages to or theft of any personal device

9.4.8 Must be in good working condition and have the most recent anti-virus software installed.

9.4.9 When handheld devices like cellphones, iPhones, Blackberrys, iTouch or other electronic devices are confiscated from a learner, the following sanctions will apply:

9.4.9.1 1st Offence: The device will be confiscated, parent(s) / guardian(s) will be contacted and will be required to retrieve the device from the school. Refer to Schools Code of Conduct with regard to protocol.

9.4.9.2 2nd Offence: The device will be confiscated, parent(s) / guardian(s) will be contacted and will be required to retrieve the device from the school. The device will be removed from the network for a period of one week. A final warning letter will be issued.

9.4.9.3 3rd Offence: The device will be confiscated for a period of 3 months, parent(s) / guardian(s) will be contacted and will be required to retrieve the device from the school. The learner, accompanied by his / her parent(s) / guardian(s) will be required to attend a disciplinary hearing. See School Code of Conduct.

Failure to abide by this Policy, as with other policies at Rylands High School High School, may result in disciplinary action as described in the school's Code of Conduct and School Rules.

10 STORAGE OF DOCUMENTS

10.1 Learners are provided with network locations in which to store documents and these locations are provided solely for storing school-related documents. These locations may not be utilized to store any personal information.

10.2 In particular, no personal photos, music and video clips may be stored on any part of the ICT System without the approval of RYLANDS HIGH SCHOOL.

11 MONITORING

11.1 As part of the continuing effort to protect learners when using the ICT System and personal devices, and to ensure learners have a positive and safe experience, the user must

acknowledge that RYLANDS HIGH SCHOOL and its representatives may monitor, access, examine and intercept any communication on or via any component of the RYLANDS HIGH SCHOOL ICT System or personal devices, by human or automated means. For such purpose, RYLANDS HIGH SCHOOL has software that is designed to monitor each learner's use of the ICT System, all his/her communications and all usage of personal devices when connected to the RYLANDS HIGH SCHOOL Wi-Fi.

11.2 Learners shall have no expectation of privacy when utilizing any component of the ICT System.

11.3 Learners shall co-operate with RYLANDS HIGH SCHOOL to enable such access, and review, including providing any necessary passwords. Failure to co-operate with RYLANDS HIGH SCHOOL in this way may result in disciplinary action being taken.

11.4 RYLANDS HIGH SCHOOL may from time to time need to appoint external investigators and/or experts for the purposes of conducting forensic and other investigations into unlawful use and/or access to the ICT systems and/or unlawful activities using the ICT Systems. Such external investigators and/or experts may need to access Learners' communications and/or the ICT system. No investigator/expert shall be granted access to any communications and/or ICT systems, except for the sole purpose of conducting an audit/investigation as described/indicated in this clause.

12 DISCIPLINARY PROCESS

12.1 Breach of this guideline may result in disciplinary action.

12.2 If you think you have breached the guideline, please notify a teacher or the ICT support staff immediately so the school can take the proper steps to help minimize the impact it may have.

13 BREACH

Where a breach or a disregard of this guideline has occurred, appropriate disciplinary action will be taken in line with the relevant SCHOOLS NETWORK policies.

14 GUIDELINE EFFECTIVE DATE

The guideline will be effective on the date on which it is signed by the relevant authority.

15 Appendix – Definition of Terms

Agents: A new type of software that performs special tasks on behalf of a user, such as searching multiple databases for designated information.

Confidential information: A designation for information, the disclosure of which is expected to damage SCHOOLS NETWORK or its business affiliates.

Critical information: Any information essential to SCHOOLS NETWORK business activities, the destruction, modification, or unavailability of which would cause serious disruption to SCHOOLS NETWORK business.

Data Security Classification: The reference to "sensitive" data refers to the classification of SCHOOLS NETWORK data into two basic categories:

SCHOOLS NETWORK Proprietary is information pertaining to business operations, new products, techniques, proposals or related information which, if compromised, would seriously impair SCHOOLS NETWORK operations.

SCHOOLS NETWORK Private is information pertaining to business operations or individuals, and is of such importance to the SCHOOLS NETWORK, or is so personal in nature, that indiscriminate release would have adverse effects on the SCHOOLS NETWORK or the employee involved. Privileged employee information such as salaries and personnel records such as change requests is typical of SCHOOLS NETWORK Private.

Default password: An initial password issued when a new user-ID is issued, or an initial password provided by a computer vendor when hardware/software is first delivered.

Downloading: The transfer of data from a host computer (mainframe, minicomputer, network server, etc.) system to a connected workstation, such as a personal computer.

End-user: A user who employs computers to support business activities, who is acting as the source or destination of information flowing through a computer system.

Extended user authentication technique: Any of various processes used to bolster the user identification process achieved by user-IDs and fixed passwords (see hand-held tokens and dynamic passwords).

Firewall: A logical barrier stopping computer users or processes from going beyond a certain point in a network unless these users or processes have first passed some security check (such as providing a password).

Information retention schedule: A formal listing of the types of information that must be retained for archival purposes and the timeframes that these types of information must be kept.

Log-in banner: The initial message presented to a user when he or she first makes connection with a computer.

Log-in script: A set of stored commands which can log a user into a computer automatically.

Master copies of software: Copies of software which are retained in an archive and which are not used for normal business activities.

Password guessing attack: A computerised or manual process whereby various possible passwords are provided to a computer in an effort to gain unauthorised access.

Password reset: The assignment of another (temporary) password when a user forgets or loses his/her password.

Password-based access control: Software which relies on passwords as the primary mechanism to control system privileges.

Password: Any secret string of characters used to positively identify a computer user or process.

Positive identification: The process of definitively establishing the identity of a computer user.

Privilege: An authorised ability to perform a certain action on a computer, such as read a specific computer file.

Restricted Area: An area in which sensitive information is being processed or worked and therefore requires physical access controls.

Restricted information: Particularly sensitive information, the disclosure of which is expected to severely damage SCHOOLS NETWORK or its business affiliates (see confidential information).

Screen saver: A computer program that automatically blanks the screen of a computer monitor, CRT, LCD, Plasma after a certain period of no activity.

Security patch: A software program used to remedy a security or other problem (commonly applied to operating systems).

Sensitive information: Any information, the disclosure of which could damage SCHOOLS NETWORK or its business associates. Any data labelled as SCHOOLS NETWORK secret or SCHOOLS NETWORK top secret.

Shared password: A password known by and/or used by more than one individual.

Special system privilege: Access system privileges allowing the involved user or process to perform activities which are not normally granted to other users.

Suspending a user-ID: The process of revoking the privileges associated with a user-ID.

Systems administrator: A designated individual who has special privileges on a multi-user computer system, and who looks after security and other administrative matters.

Uploading: The transfer of data from a connected device, such as a personal computer, to a host system (mainframe, minicomputer, server, etc.).

User-IDs: Also known as accounts, these are character strings that uniquely identify computer users or computer processes.

Valuable information: Information of significant financial value to Parliament or another party.

Verify security status: The process by which controls are shown to be both properly installed and properly operating.

Virus: A parasitic software program, equipped with the means of reproducing itself, that spreads throughout a computer or network by attaching itself or infecting other software or diskettes. A worm is a similar program that propagates across a network by making copies of it.

Virus screening software: Commercially-available software that searches for certain bit patterns or other evidence of computer virus infection.

BYOD Bring Your Own Device

_____	_____	_____
IT Committee	**SGB Chairperson**	**Principal**

_____

Date: