SPRINGFIELD CONVENT - IT POLICY

Contents

Asset Management

All IT equipment is documented electronically. This document forms part of the School asset register. All old/ failed/ obsolete equipment is disposed of responsibly (E-Waste facility), the disposal process comprises of the following:

1) Identify equipment to be disposed of
2) IT Department serial tags equipment to be disposed of
3) Lee Bassett confirms list and signs-off equipment, removes equipment off asset register
4) Garth Andrews takes equipment to E-Waste facility

Backup Strategy

The Springfield network comprises a Client-Server topology. There are Central Servers which hold the Schools data (Staff/ Student). These Servers are backed up daily onto a Network Attached Storage Device (NAS) which is located on the School Campus but not near the Servers. Backups are checked/ monitored regularly. iTechSolutions are responsible for the Backup Process.

Resource	**Note**	**Backup Location**	**Frequency**
Email	Office 365	Cloud Based – Microsoft	Daily
File Server	Student/ Staff Resources	Local Backup	Daily
Accpac/ Admin/ Pastel/ Edadmin	Accpac/ Pastel/ Admin Files/ Secretary Files	Local Backup – Admin/ Pastel/ Edadmin Cloud Backup - Accpac	Daily
Active Directory	Student/ Staff usernames	Local Backup	Daily

Staff and pupils are expected to save their information in the respective locations on the School Network i.e H Drives/ Staff Common etc

Staff and Pupils have access to Cloud storage (One Drive for Business and Google Drive). This provides a safe mechanism for working on documents out of the School Network.

Disaster Recovery

iTechSolutions has documented the School Network/ Configuration information. In the event of destruction whether in full or part data can be retrieved from backup/ archive. New equipment would need to be procured.

Offsite storage facility to replicate school's data for restoration for non-critical data ie: Staff & Students files on a monthly replication schedule.

Resource/ Impact:

1) Email
    a. Cloud based – no impact
2) Phone System
    a. Cloud based – limited impact
    b. Macrolan to facilitate softphones (software based) on new equipment
3) File Servers
    a. File Access – large impact. New hardware procurement. Restoration from backup/ archive
4) Edadmin
    a. Parent/ Student/ Staff Information – limited impact. New hardware procurement. Restoration from backup/ archive.
    b. Interim measure to utilise Hosted Server (iTechSolutions Hosted Environment)
5) Accpac/ Pastel
    a. Financial Data – limited impact.
    b. Interim measure to utilise Hosted Server (iTechSolutions Hosted Environment)

Data Management

Each member of the Springfield Network community is allocated network space

Students

1) Email/ Cloud Storage – 15 GB
2) H Drive – 1 GB
3) Student Grade Drives – 25 GB (Grade Share)

Staff

1) Email – 50 GB
2) Cloud Storage – 1 000 GB
3) H Drive – 10 GB
4) Staff Drive – 50 GB (additional space is allocated depending on requirement)

Network Security

1) Springfield utilises Microsoft Server– Active Directory. The Server infrastructure adheres to current product lifecycle (https://support.microsoft.com/en-us/gp/lifeselectserv)
    a. All staff/ students have a unique username/ password and are encouraged to refresh their passwords on a frequent basis
2) Access to resources (machines/ files/ folders) is based on Industry Standard "least privilege". Appropriate access to perform their function
3) WiFi Access codes are refreshed on a monthly basis and usage closely monitored
4) Logon/ logoff information is logged
5) Internet access is logged
    a. All Internet access is filtered through a Cyberoam UTM Device
    b. Access is logged
    c. Filters are in place for staff/ students
    d. Any in-appropriate behaviour is logged and addressed with Management
6) Email communication logs are logged (sender/ recipient/ date/ time)
7) Appropriate permissions are in place to safeguard sensitive data (HR, financial, Edadmin)
8) All machines have anti-virus/ anti-malware software installed to prevent malicious damage to data and Application Filters applied to prevent illegal downloading of content from the internet into the School's network
9) The network is segmented utilising VLAN topology. Guest/ WiFi networks are unable to gain access to the Schools Data network.

Data Archiving

1) All electronic Financial/ Administration information to be kept for a minimum period of 7 years
2) Student/ Staff H Drives to be kept for 1 (one) year after leaving
3) All digital information to be archived on an onsite Network Attached Storage Device (NAS) which is in addition replicated to the DR (Disaster Recovery) site

Data Security

1) Least privileged concept is adopted whereby the required permissions needed to perform job are assigned
2) All data to be shared on Microsoft Windows Server utilising NTFS permissions
3) All School owned mobile machines (laptops) are to be secured with BITLOCKER

IT Usage Policy

Policy: Access to the Internet through the School is a privilege. Users who are granted this privilege must adhere to strict guidelines concerning the appropriate use of this information resource. Users who violate the provisions outlined in this document are subject to disciplinary action. In addition, any inappropriate use that involves a criminal offence will result in legal action. All users are required to acknowledge receipt and understanding of the guidelines contained in this document.

Scope: This policy applies to all staff and pupils who have access to Internet and related services through the School network infrastructure. Internet related services include all services provided with the TCP/IP protocol, including but not limited to Electronic Mail (e-mail), File Transfer Protocol (FTP), Gopher, and World Wide Web (WWW) access.

Procedure:

1) ACCEPTABLE USE

a. Access to the Internet is specifically limited to activities in direct support of official School business.

b. In addition to access in support of specific work related duties, the School Internet connection may be used for educational and research purposes.

c. If any user has a question about what constitutes acceptable use he/she should check with school management for additional guidance. Management or supervisory personnel shall consult with the Information Services Manager for clarification of these guidelines.

2) INAPPROPRIATE USE

a. The School Internet access shall not be used for any illegal or unlawful purposes. Examples of this would be the transmission of violent, threatening, defrauding, pornographic, obscene or otherwise illegal or unlawful materials. Users may not express racist or sexist sentiments, or any other form of negative or derogatory speech.

b. The School electronic mail or messaging service should be for School business only. Limited personal use will be allowed at the discretion of School Management. These services shall not be used to harass, intimidate or otherwise annoy another person. This includes “flaming” and/or bombing a friend or colleague with junk mail as well as sending chain letters.

c. Users may not attempt to create or introduce any form of virus onto the network.

d. Users may not load (off CD, DVD or flash disk) or download any software or data files onto the network without the express permission of the IT Department. This includes photos, “patches”, “cheat codes” or games of any nature.

e. The School Internet access shall not be used for private, recreational or other non-School related activity. Limited personal use will be allowed at the discretion of School Management.

f. The School Internet connection shall not be used for commercial or political purposes.

g. Use of the School Internet access shall not be used for personal commercial gain. Internet access shall not be used for performing work for profit.

h. Users shall not attempt to circumvent or subvert security measures on the School's network resources or any other system connected to or accessible through the Internet.

i. School users shall not use Internet access for interception of network traffic for any purpose unless engaged in authorized network administration.

j. School users shall not make or use illegal copies of copyrighted material, store such copies on School equipment, or transmit these copies over the School network.

3) INTERNET AND E-MAIL ETIQUETTE

a. Users shall ensure that all communication through School e-mail or messaging services is conducted in a professional manner. The use of vulgar or obscene language is prohibited.

b. School users shall not reveal private or personal information without specific approval from management.

c. Users should ensure that e-mail messages are sent only to those users with a specific need to know. The transmission of e-mail to large groups or messages with large file attachments should be avoided.

d. Electronic Mail is not guaranteed to be private. Messages transmitted through the School e-mail system or network infrastructure are the property of School and are therefore subject to inspection.

4) SECURITY / PRIVACY

a. School users who identify or perceive an actual or suspected security problem shall immediately contact the School Information Systems Manager.

b. Users shall not reveal their account password or allow another person to use their account. Similarly, users shall not use the account of another user.

c. Access to School network resources shall be revoked for any user who might be identified as a security risk or has a demonstrated history of security problems.

d. Users shall not attempt to access any communication, file or other information belonging to any other user of the network.

e. Users must inform the IT Department if they accidently discover confidential or undesirable material.

f. Users may not attempt to discover the password of any other user, by any means whatever.

5) SAFETY

a. Users may not reveal their own, their friends' or their teachers' personal addresses or telephone numbers on the Internet.

b. If an incoming communication asks for more personal information than the user cares to reveal, or makes the user feel uncomfortable in any way, said user must inform the IT Department immediately.

c. Do not send any banking details over the internet

6) PENALTIES

a. Any user who violates this policy is subject to the loss of network privileges and any other School disciplinary actions deemed appropriate.

7) USER COMPLIANCE

a. All terms and conditions as stated in this document are applicable to all users of the network and the Internet connection.

b. All users must agree to abide by this policy by signing the Internet Use Agreement form.

Protection of information

All staff are responsible for safeguarding the Schools information whilst utilising the School Network, responsibilities include but aren't limited to:

1) Not revealing username/ passwords
2) Logging off/ locking workstation when leaving
3) Ensure appropriate permission has been obtained/ granted for downloading/ uploading information onto School Network (files/ folders/ software)
4) Only software purchased/ licensed to the School may be installed

Software Security

Springfield utilises the "least privilege" principle whereby appropriate access is given to perform one's function. iTechSolutions are responsible for installing/ maintaining software and to ensure compatibility.