Marian College Ararat

IT Network/Security Policy

Contents

1. Overview

This policy outlines the policies and procedures in place to maintain and safeguard the College's computer network infrastructure and data. This includes physical security, cyber security and inappropriate use.

This policy does not cover the College's internet site which is managed by a third party external to the College, nor does it cover other third party systems used by the College and hosted external to the College.

For the purposes of this policy the core components of the College network are as follows:

- Infrastructure. The College maintains an internal network consisting of Servers, Switches, fibre cables, wireless access point and user devices.
- SIMON. This database is used by the College to record and manage student and curriculum information
- SAS/PAY3K. This system is used to manage the College Financial and HR information and contains the parent and student records that are also used by SIMON.
- Internet Access. Students and staff are provided with access to the internet commensurate with what they need for the purposes of the College. In recent years the trend towards cloud storage Google education tools and electronic books good tools has mean that internet access has become a critical component of the College. This trend has also meant that there is a decreasing reliance on College provided storage.
- Other Systems. There are number of other systems running on the Colleges network such as CCTV and the Library Catalogue system. These are less critical that the components listed above.

2. Physical Security

IT Infrastructure.

IT Infrastructure assets are located within the College and as such must be secured via physical means such as locked doors and as part of the general College security arrangements such as out of hours security monitoring and patrols.

College servers are contained in a dedicated air-conditioned room which must be physically restricted to IT staff. All servers must have a back-up power supply (UPS) capable of maintaining them for a period of 20 minutes in the event of a power failure. At lease one of the UPS's must have a function capable of alerting IT staff in the event of power being lost in the server room.

The College also contracts an outside expert organization to constantly review its network and provide advice on design, security and maintenance issues.

IT Equipment on Personal Issue

IT equipment such as personal devices or laptops issued to staff and students must be recorded by the IT Department. Both staff and students issued with IT equipment must sign an agreement covering care and use.

Part 8 lists the user agreements relating to the issue of IT equipment to individuals.

3. System Security

System security is to be managed such that access to the Colleges IT systems is restricted so that only authorized users have access and such access is limited to the role and function of the user. This security is to reinforced through a range of measures including:

- **Patching.** The IT manager must ensure that all server system patches are applied within 2 weeks of them being released. System patches are to be independently audited by the external party providing expert assistance at least annually. Laptop and other devices owned or manage by the College should be set to automatically process critical updates.

- **Firewall.** The College must maintain an effective Firewall system capable of managing external access to College IT systems and the internet. This must be a reputable commercial system that is also capable of providing internet filtering suitable for a student environment.

- **User Access.** Access to the College IT systems must be managed through the access levels granted to users and should correspond to the role or function the user undertakes. The following table provides a template for access within the College:

Folder Access	Student	Teacher	Admin	IT Dept	Guest
Home Folder	Y	Y	Y	Y	
Student Shared Work	Y	Y	Y	Y	
Teacher Shared Work		Y	Y	Y	
Admin Folder			Y	Y	
System Access				Y	
Internet Access	Student Access	Teacher Access	Teacher Access	Teacher Access	Student Access

Note : Student Internet access differs from Teacher access in that it is filtered differently and is generally more restricted.

Access to the College systems (granting and revocation) is managed the IT department and is implemented as follows:

- **Teachers and Admin staff.**Creation/Revocation of staff users will be authorised by the HR Manager once staff have signed an employment contract. Generally, such access is not activated until the staff physically commenced at the College.

- **Students.** Access is granted and revoked based on the status of the student in SAS system. In practice this is undertaken automatically by a software program based on the Student records in SAS.

- **Guests.** Guest access is granted and revoked manually by the IT Dept upon request by a staff member.

- **Access to E-mail.** The College uses Google e-mail (gmail) which is external to College systems, however, as part of Google Education it is administered by the IT Dept. Student access and revocation is undertaken automatically based on SAS student records. Teacher and Admin staff e-mail is managed manually based on advice from the HR Manager, however, access may be created prior to a

teacher/admin person physically starting work at the College if requested by a Leadership member or Faculty head.

- **Access to Core Systems.** Access is dependent on access to the general College system and is managed by the System Administrator of each system. Specifically:
    - SIMON. Access is managed by the Student Secretary
    - SAS. Access is managed by the Business Manager.
- **Password Policy**. Where possible the College will aim to implement a single sign-in with a standard password policy. The exception to this is the SAS system which has limited users and subject to other access restrictions. The minimum standards for passwords for access to the College network are as follows:
    - Password Length : Minimum of 8 characters.
    - Password Composition : Must have at least one alphabetic or numeric number.
    - Number of unsuccessful trials before account locked : 5
    - Password history retention : 24

    The IT Department must enforce a password change at least twice per year.
- **Virus Protection.** The IT manager must ensure the College system runs an effective Anti-Virus system. Any such system must be capable of running continuously and be regularly updated to ensure that new and emerging threats are protected against. Such a system must also maintain log files capable of recording potential system attacks. The IT Manager must institute procedures to ensure the anti-virus system is in continued operation.

4. IT Usage Policy

As a general principle the Colleges IT systems are for the purposes of running the College and providing educational resources to students and teachers. Limited personal use is permitted, however, the College must ensure that it has adequate policies or procedures in place clarifying such usage to Staff and Students.

5. System Maintenance/Replacement

In conjunction with the Business Manager the IT Manager must ensure that there is a structured replacement/improvement program to ensure that core infrastructure is able to meet the needs of the College. As a general rule core infrastructure (Servers and core switch) should be replaced before the end of their warranty period. If equipment is retained longer, consideration should be given to extending warranties.

The IT Manager is to ensure there is a formal system staff can use to report hardware and software issues. Such a system must record the outcome of the issue and the date it was resolved.

The Business Manager is to ensure that at independent network review is undertaken at least every three years to identify any weaknesses or improvement opportunities.

6. Data Backup.

As a general principle all data files and servers should be backed up as follows:

- All files and servers, including core systems, backed up daily. Where possible the back-up should also be stored on a server in a separate physical building.
- Fortnightly back-ups of core systems (SAS/SIMON) should be held off site. Back-ups of these systems should also be undertaken and stored off site at the end of school terms and after triggers points, such as before and after roll-overs, and at the end of reporting periods.

7. System Continuity.

The IT Manager and Business Manager are responsible for ensuring that there are plans in place to manage system outages ranging from simple equipment failures up to catastrophic disasters such as the physical destruction of the College servers. Appendix A provides a summary of likely issues and approaches to continuing the continuity of the network.

8. Associated Documents.

- Staff ICT Agreement
- Student Device User Agreement
- Student BYO Laptop Agreement
- Acceptable Use Agreement - Student

APPENDIX A

Network Continuity Plans

The College IT network faces a number of potential threats capable of crippling it or reducing its performance. In general, these can result from:

- **Loss or damage to internal infrastructure.** The College aims to reduce the impact of this type of threat through a range of measures including :
    - Operating a virtual server environment
    - Maintaining spare equipment
    - Maintaining agreements with equipment/server suppliers that specify response times
    - Data back-ups
    - Making greater use of Cloud services for teacher and student resources.
    - Agreement with St Mary's primary school that we could use their infrastructure to operate core systems.
    - Maintain a mirror site in a physically separate building (Brigidine Centre).

- **Loss of power or internet connection.** The College aims to reduce its exposure to these types of outages through a range of measures including:
    - Diversifying its power connection through three separate power connections into the College.
    - Implementing a second, separate, internet connection into the College (expected 2019 when the NBN reaches the College)

- **Cyber Attack/Hacking.** The College aims to reduce its exposure and the impact of such attacks through a range of measures including:
    - Using a specialized third party provided and managed firewall system
    - Operating an effective anti-virus application
    - Progressively moving traditional school-based data and applications to third party cloud services.
    - Employing outside specialists to design and provide advice and support to our network and IT staff.
    - Staff/Student education.