Maronite College of the Holy Family

Information Communications & Technology (ICT) Policy

Maronite College of the Holy Family policies have a commitment to Maronite Catholic ethos and values and should be read in conjunction with other policies and procedures and with relevant legislation.

POLICY REVIEW

The policy will be reviewed not less frequently than once every three years.

POLICY DATES			
Implemented	August 2013	***Reviewed***	23/9/19
Next Review Due	November 2022		
POLICY AUTHORISATION			
Sr Irene Boughosn **PRINCIPAL**			
POLICY DETAILS			
Policy Number: 0028 Policy Version: 0001			

OBJECTIVE OF ICT AT MCHF COLLEGE

Maronite College of the Holy Family aims to educate staff, students and the wider community to use ICT effectively to support and develop their lifelong learning.

1. VISION

1.1 To use ICT as an effective and efficient teaching, learning and management tool throughout the College.
1.2 To continuously improve the ICT capability of students and staff.
1.3 To provide access to high quality ICT resources and support for staff and students.

2. DEFINITIONS

'Staff' means employees, volunteers and contractors who use ICT for the purpose of work within the College.

'ICT' means information and communications technologies and includes computers, mobile phones, PDAs, iPads, internet and network services, portable data storage devices, online data storage mediums, telephones, printers, fax machines and all other digital communications devices used at the College.

'Social media' means web-based and mobile technologies which turn communication into interactive dialogue. Examples include but are not limited to Facebook, YouTube, Instagram, Snap Chat, Twitter, blog or wiki posts and comments.

'BYOD' refers to Bring-Your-Own-Device. The term *'device'* refers to any mobile electronic technology, including assistive technologies, brought into the College, which is owned by the member of staff or the student, and which has the capability of connecting to the College's Wi-Fi network.

3. MEMBERS OF THE ICT COMMITTEE

- Sr Irene Boughosn – Principal
- Mr Elie Asmar – Head of Secondary
- Ms Rupa Bala – Business Manager
- Mr Dean Day – Head of Primary
- Ms Georgette Dalla – Director of Curriculum
- Ms Zeina Sharbeen – eLearning Coordinator & ICT Charirperson
- Secure Agility Representative

3.1 Managing Director of Secure Agility (external company responsible for providing IT support) has regular meetings with the College Principal and Business Manager to assist with strategic planning and development of ICT matters across the College.

3.2 The ethos of the College and the ICT Committee is of team work and co-operation. This is achieved through reviews and a shared goal to improve standards of resources and support for the curriculum and beyond.

3.3 Monitoring of the ICT policy is the responsibility of the ICT Committee of the College. The policy is reviewed no less than every 3 years by the ICT Committee.

4. WHOLE-COLLEGE APPROACH

4.1 The College's policy is to use and develop the opportunities provided by ICT to benefit the entire 'learning community.' This includes communicating with parents; supporting students' learning both at the College and at home; and encouraging lifelong learning across the local community.

4.2 ICT is increasingly used to support liaison and transfer of information. The College website (www.mchf.nsw.edu.au) and Skoolbag app give relevant information about the College to parents, guardians and students. Following approval by the Principal, updates are made to the main College website. Furthermore, updates are made to the Skoolbag app as required.

4.3 The developing use of ICT to enhance teaching and learning is one of the key areas of focus of the ICT Committee. This vision is passed onto Coordinators and staff when Professional Development is offered so that there is a whole College approach to the development of ICT in teaching and learning.

4.4 ICT staff continue to review all teaching and learning in line with current good practice. National strategies and initiatives are incorporated into schemes of work and pedagogy as appropriate for our students.

4.5 Core ICT lessons allow all students opportunities to develop their ICT skills in Digital Technology, with further opportunities to achieve ICT related qualifications as they progress throughout their academic careers.

4.6 A policy of integrating ICT into teaching and learning across the curriculum is reflected in the ongoing provision of digital projectors, television screens, interactive whiteboards and BenQ Boards in classrooms.

5. STUDENT RIGHTS & RESPONSIBILITIES

5.1 All students are entitled to access ICT resources, throughout all subjects studied from K-12. Several departments also ensure that pupils have access to ICT resources in their subject areas through, but not limited to Moodle, OneNote, OneDrive and SharePoint.

5.2 Student progress in ICT is assessed against NESA criteria and implemented in line with whole College assessment, recording and reporting guidelines. Students are encouraged to use self-assessment along with targets to improve performance and progress.

5.3 As an inclusive community at the College, it is important that ICT is used effectively and appropriately to support access to the curriculum for all students.

6. STAFF RIGHTS & RESPONSIBILITIES

6.1 All staff are encouraged to further improve their skills and ICT capability. In addition, they have a responsibility to keep abreast of developments in ICT. Various Professional Development opportunities will be conducted by qualified staff at MCHF to assist with the learning of new applications or to enhance knowledge of current applications. Staff are also encouraged to complete Teacher Training Australia (TTA) online courses to assist with their skill development.

6.2 Staff have access to various websites set up specifically to support the effective use of ICT in the classroom including the College's Learning Management System (LMS), Moodle.

6.3 Staff have access to student information via the School's Information Management System from various classrooms and offices.

6.4 The College uses electronic registration to improve student attendance and track behaviour. Attendance and lateness are regularly reviewed by staff and suitable action taken to reduce instances of lateness or truancy.

6.5 Staff are expected to use ICT based applications to record Academic Progress. This can then be used by KLA Coordinators to set and review development targets.

6.6 Staff use electronic assessment procedures to record and report on student progress.

7. BYOD RIGHTS & RESPONSIBILITIES

7.1 BYOD Requirements

7.1.1 MCHF allows staff to bring devices to the College for the purposes of planning and curriculum implementation.
7.1.2 MCHF allows students to bring devices to the College for the purpose of learning.
7.1.3 Use of devices at College will be governed by College-developed policies that involve College-community consultation.
7.1.4 While implementing BYOD, MCHF provides information to key community stakeholders including teachers, parents, guardians and students.
7.1.5 Staff must complete and return a signed BYOD Staff Agreement prior to participation in BYOD.
7.1.6 Students and their parents/guardians must complete and return a signed BYOD Student Agreement prior to participation in BYOD.
7.1.7 The College will choose the BYOD model that is relevant and appropriate for the needs of the staff, students and the community.
7.1.8 While implementing BYOD, the College has considered strategies to ensure that all staff and students are able to engage fully in classroom activities. This includes strategies to accommodate both staff and students without a device

7.2 Acceptable Use of Device

7.2.1 The Principal will retain the right to determine what is, and is not, appropriate use of devices at the College within the bounds of the ICT's policies and limitations.

7.2.2 Staff and students must comply with College policies concerning the use of devices at the College while connected to the Wi-Fi network.

7.2.3 Mobile Phones and Smart Watches are not permitted to be accessed by students during College hours. Students accessing mobile phones or smart watches will be disciplined in line with the Discipline Policy outlined in the College Student Development Policy. The College will take NO responsibility for any damaged, lost or broken mobile phones or smart watches. Students needing to access mobile phones during the College day must be supervised by a teacher.

7.2.4 Staff and students must not attach any College-owned equipment to their mobile devices without the permission of the College Principal, an appropriate Coordinator or a Secure Agility representative.

7.2.5 Staff and students must not create, transmit, retransmit or participate in the circulation of content on their devices that attempts to undermine, hack or bypass any hardware and software security mechanisms that have been implemented by the College or its Information Technology Directorate.

7.2.6 Staff and students must not copy, transmit or retransmit any material that is protected by copyright, without prior permission from the copyright owner.

7.2.7 Staff and students must not take photos or make video or audio recordings of any individual or group without the express written permission of each individual (including parent/caregiver consent for minors) being recorded and the permission of an appropriate coordinator.

7.2.8 Staff and students are prohibited from using the College's network services to seek out, access, store or send any material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature. Such use may result in disciplinary and/or legal action.

7.2.9 Staff, students and their parents/guardians are advised that activity on the internet is recorded and that these records may be used in investigations, court proceedings or for other legal reasons.

If MCHF has reasonable grounds to suspect that a device contains data which breaches the BYOD Student Agreement, or BYOD Staff Agreement, the Principal (or delegate) will confiscate the device for the purpose of confirming the existence of the material. Depending on the nature of the material involved, College disciplinary action may be appropriate or further action may be taken including referral to the police.

The consequences of any breaches of the College's ICT policy will be determined by the Principal in accordance with relevant College policies and procedures and accepted College practice.

7.3 Staff Agreement

MCHF ensures that staff is aware of and agree to, their obligations under the College's ICT policy through the BYOD Staff Agreement. MCHF will retain a copy of the BYOD Staff Agreement in print or electronic form and it will be kept on file with your staff record.

7.3.1 Prior to connecting devices to the College's Wi-Fi network, staff must return the signed BYOD Staff Agreement.

7.3.2 The BYOD Staff Agreement contains both BYOD Device Requirements and BYOD Staff Responsibilities.

7.3.3 By accepting the terms of the BYOD Staff Agreement, staff acknowledge that they:

- agree to comply with the conditions of the College's BYOD policy; and
- understand that noncompliance may result in disciplinary action.

7.4 Student Agreement

MCHF ensures that students and their parents/guardians are aware of and agree to, their obligations under the College's ICT policy through the BYOD Student Agreement. MCHF will retain a copy of the ICT Student Agreement in print or electronic form and it will be kept on file with your student record.

7.4.1 Prior to connecting devices to the College's Wi-Fi network, students must return the BYOD Student Agreement.

7.4.2 The BYOD Student Agreement contains both BYOD Device Requirements and BYOD Student Responsibilities.

7.4.3 The BYOD Student Agreement must be signed by the student and by a parent/caregiver. If a student is 18 years of age or more, there is no requirement to obtain the signature of a parent/caregiver. Principals (delegate) will make these determinations.

7.4.4 By accepting the terms of the BYOD Student Agreement, the student and their parents/guardians acknowledge that they:

- agree to comply with the conditions of the College's BYOD policy; and
- understand that noncompliance may result in disciplinary action.

7.5 Care and Support

Staff and students and their parents/guardians are solely responsible for the care and maintenance of their devices.

7.5.1 Staff and students must have a supported operating system and current antivirus software installed on their device and must continue to maintain the latest service packs, updates and antivirus definitions as outlined on this BYOD Policy document.

7.5.2 Staff and students are responsible for ensuring the operating system and all software on their device is legally and appropriately licensed.

7.5.3 Staff and students are responsible for managing the battery life of their device. Staff and students should ensure that their devices are fully charged before bringing them to the College. MCHF is not responsible for providing facilities for staff and students to charge their devices.

7.5.4 Staff and students are responsible for securing and protecting their device at the College, and while travelling to and from the College. This includes having a protective/carry case and exercising common sense when storing your device. The College is not required to provide designated or secure storage locations.

7.5.5 Staff and students should clearly label their device for identification purposes. Labels should not be easily removable.

7.5.6 Staff and students should understand the limitations of the manufacturer's warranty on their devices, both in duration and in coverage.

7.5.7 Staff and students bring their devices onto the College site at their own risk.

7.5.8 In cases of malicious damage or theft of a staff member or student's device, existing Discipline Policy for damage to College or personal property apply.

7.5.9 MCHF is under no obligation to provide technical support for hardware or software. The College may choose to provide this service to staff and students if there are sufficient resources available in the College.

7.5.10 Staff and student devices are not covered by the College's Insurance policy. Insurance is the responsibility of staff, parents/guardians and students.

8. ACCEPTABLE USE OF SOCIAL MEDIA

8.1 Staff and students must, at all times, behave in an ethical manner when using social media.

8.2 Engagement in social media should be for the purposes of collaboration, communication and engagement within an educational/learning context, as well as community engagement in a marketing context.

8.3 Staff should always remain aware of their professional responsibilities, even when using their personal social media accounts.

8.4 Students must always remain aware of their responsibilities when using their social media accounts. This includes and is not limited to posting images/video on social media sites (including Facebook, Snap Chat, Twitter, Instagram etc) that may put the College or other students or teachers into disrepute. The College can involve the police should they deem the online activity to have broken the law.

8.5 Staff personal social media use must be congruent with the professional standards expected of an employee of the College.

8.6 State and Federal legislation and the child protection protocols and policies of the College must always be observed.

8.7 The Principal is to approve any local use of social media in line with this policy.

8.8 The relevant age limits for students using social media platforms must be strictly observed. The College must ensure that students have the necessary parental permissions before they can engage in the use of social media.

8.9 Creation of College social media account for a College team or specific project can only be done with the approval of the Head of Primary or Head of Secondary.

8.10 When staff members are using social media in a professional context, an account must be created specifically for this purpose. Personal social media accounts should be for personal use only.

8.11 Staff members must respect student's right to privacy, consistent with the relevant laws and regulations and student and parent choice.

8.12 Students must respect the College and teacher's right to privacy, consistent with the relevant laws and regulations and College policies.

9 NETWORK AND RESOURCES

9.1 Network Access

9.1.1 Staff and students have access to reliable and industry-standard hardware and software in order to use ICT effectively as a teaching and learning resource, and as a working tool for management and administration.

9.1.2 Staff and students have access through the College's network to their personal data areas (Microsoft OneDrive), shared data (Microsoft SharePoint), both local and networked applications and the internet.

9.1.3 Network access is via a secure login. Passwords are to be kept confidential and used only by the person to whom they were allocated.

9.1.4 The Administrative network, which is managed by the Business Manager, allows staff access to information for electronic student data, timetables and attendance, and also includes the College's financial management system.

9.2 ICT labs are allocated for use by supervised classes as follows

9.2.1 Primary Core ICT lessons and Secondary IT specialty subjects are timetabled in the College timetable.

9.2.2 Secondary bookings of ICT labs can be arranged through the shared room booking document on SharePoint. Primary can borrow additional laptops and iPads from the Primary Learning Centre.

9.3 Network Security

9.3.1 Computers in ICT labs must be monitored by teachers within the classroom.

9.3.2 To maintain network security, the wireless access points that are in use around the College use WPA2 encryption.

- To ensure security, only selected staff have access and can update the College Facebook page, the College Newsletter, Skoolbag App, College Website, and Electronic Board

9.3.3 System Center Endpoint Protection Anti-Virus/Anti Malware is installed on every networked computer. The software updates itself daily, and constantly scans for viruses to keep the network secure.

9.3.4 All parents enrolling students from Kindergarten to Year 6 are informed of the College's Internet Acceptable User Policy via the Enrolment Form. Upon entering Secondary, new enrolments in Years 8-12 and all Year 7 students along with their parents/guardians are required to sign an ICT Agreement. If the agreement is not completed and returned, student's internet/network access will be withdrawn.

9.3.5 Internet content is controlled primarily by the College using web filtering software/firewall *Palo Alto*.

9.3.6 In order that network security is maintained, staff are asked to change their passwords regularly and computers logged in as a member of staff, will automatically 'lock' after an appropriate period of inactivity.

9.3.7 Student's network access can be blocked at the discretion of the Primary or Secondary Leadership Team in the event of a student 'hacking' into the network or attempting to disrupt the smooth running of the network. In the case of extreme actions taken by a student to harm the ICT resources, the Principal or Deputy Principal can suspend the student.

9.4 Technical Support

9.4.1 On-site technical support for the College network is provided during College school terms by Secure Agility technician. They are managed by the Business Manager and are responsible for the day-to-day maintenance of the network infrastructure, hardware and software owned by the College.

9.4.2 The administrative network, which includes SAS, and admin network users are supported by Secure Agility.

9.4.3 Procedures for reporting problems and for requests to the ICT technical team are designed to be clearly communicated and straightforward for staff to follow. ICT technical team respond to the request/problem within an appropriate timeframe. Staff are to use the ICT Help Desk to communicate with the technical support team.

9.4.4 The ICT inventory is incorporated within the College's asset database and is updated periodically to show current locations and other pertinent information for ICT hardware.

9.5 Software Procedures

9.5.1 An up-to-date record of all networked software and license information is kept by Secure Agility.

9.5.2 Licensing information and proof of purchase is required by the Business Manager before accepting any request to load software on to the network, or as a local application.

9.6 Sustainability

9.6.1 Technical support routines and procedures are continuously reviewed and developed to ensure the sustainability of the network infrastructure, hardware and software.

9.6.2 The College asset register provides an audit of hardware which can facilitate decisions on repair, replacement and development. The College's procedure for writing off equipment is followed.

9.6.3 The College annual budgetary cycle provides the opportunity to identify maintenance, replacement and development needs for ICT infrastructure, network services, technical support, equipment and software. The 'core' annual budgets are ICT General and Capital. Grants are used for projects identified and agreed by the ICT Committee and guided by government recommendations.

9.6.4 Before being disposed of, all ICT equipment is firstly made safe and removed from the College's register of assets and PAT testing register. Hard drives that have been used in administrative computers are either reformatted or destroyed to wipe all data, or if appropriate stored for possible reuse. Equipment is then stored in a secure location on site until there is a suitable amount for it to be removed by a registered waste removal company who issue a waste disposal receipt.

9.7 Disaster Recovery

A full back up regime is in place to back server content on back-up tapes on Monday to Friday. College related content is stored in SharePoint online. Staff emails are backed up through a third-party supplier, *Skykick*. Once a week back-up tapes are collected and stored in fire proof bags offsite by *Recall.* The backup tapes are rotated on a monthly basis. An end of month tape is also taken and placed in secure storage for six months. Application software is also backed up when new software has been loaded; server operating systems and Active Directories are backed up daily. All original software is kept separately.

In the event of a critical breakdown, the main server's warranty agreement will be activated and assistance from Secure Agility will be sought to restore normal network operations.

9.8 Emerging Technologies

In an ever-increasing world of ICT developments, it is important to keep abreast of emerging technologies and review their potential impact on teaching, learning and communication, both within the College and beyond. If a development (hardware or software) is deemed to have the potential to improve the teaching and learning, or assist administration, it will be reviewed, trialled and, if proved to be successful, incorporated into whole College use, subject to financial capacity.