ST. MARY'S *Catholic High School, Dubai*

ICT POLICY

2025-2026

St. Mary's Catholic High School, Dubai

Information and Communication Technology (ICT) department's acceptable use of ICT policy applies to all users of ICT resources.

Department ICT resources are provided to improve and enhance learning and teaching, and for the conduct of the business and functions of the Department. All users of Department ICT resources are expected to exercise responsibility, use the resources ethically, respect the rights and privacy of others. Department ICT resources should not be used for inappropriate or improper activities. This includes pornography, fraud, defamation, breach of copyright, unlawful discrimination or vilification, harassment, including sexual harassment, stalking, bullying, privacy violations and illegal activity, including illegal peer-to-peer file sharing.

The ICT department is responsible for:

- SIMS for managing school administrative information and processes
- Networking System
- Technical Resources
- Computer Lab
- Internet Services
- E-Learning Support
- Data Security and Backup
- Remote Access Control
- School Surveillance Systems – CCTV Camera
- Information Security / Cyber Security
- School Website
- Data Analysis
- Payment Gateway – Mobile Payment Service
- Technical Support

SIMS

SIMS is a management information system which provides teachers, senior leaders and support staff with tools to efficiently manage daily school life and drive improvement in schools.

The followings are supporting academic services through SIMS.

- Student Records
- Attendance
- Behavior
- Mark sheet Entry
- Programme of study tracking
- Reporting
- Summative attainment / Progress
- Formative attainment / Progress
- Timetable
- School Latest News and Updates via mobile App
- Maintain SEN Data

NETWORKING SYSTEM

School is having CISCO MERAKI cloud based well structured and secured network system with WIFI access to the students, teachers, staff and guests wherein individual policies are assigned to each user type.

TECHNOLOGY RESOURCES

The Department maintains arrangements with hardware and software suppliers so that requirements can be provided to school. The ICT department has responsibility for developing cost effective arrangements with preferred suppliers. Prior to purchasing any hardware or software, an electronic hardware/software acquisition form should be submitted to initiate the review process. A well organized purchase flow (Requisition, RFQ, Po, Approval etc.) is followed with the vendor for all purchases.

There is proper review of licensing agreements for all software. Clear expectations for maintenance, licensing, network connectivity, etc., of all hardware and software.

The ICT inventory is incorporated within the schools asset records maintained by the Accounts department, and is updated every 6 months to show current locations, and other pertinent information for all ICT hardware.

A policy of integrating ICT into teaching and learning across the curriculum has been reflected in the provision of a PC and digital projector in all classrooms and also by providing teachers with ICT access outside the main ICT rooms and classrooms. Teachers have also been provided Laptops (All new teachers have to fill in a laptop request form, which will be submitted for the Principal approval) secure network access for laptops and use the same Anti-virus software as school provided equipment. This access is maintained by the IT Support team.

COMPUTER LAB

General Use of Computer Labs:

- No food or drink at computer workstations.
- No disruptive behavior.
- No moving the lab equipment and/or cables.
- No laptops on the wired network (exception: Instructors for instructional purposes). It is okay to have laptops in the labs and be on the wireless network, they just can't be physically plugged into our jacks.
- No illegal copying of ANY materials.
- Keep sound levels to a minimum.
- The labs are for students and ICT staff ONLY. We reserve the right to check users.

a.) Students:

- Each students should login with their own active directory login ID's.
- All the files should be saved on the network drive.
- Each students should use the Pc's allotted to them by the ICT teacher.
- Printers should not be miss used.
- Bags should not been taken to the cubical.
- Any damage caused to the PC's during using should be reported to the teacher available in the LAB.

b.) IT Support:

- Creating students ID's in Active Directory.
- Maintaining servers, PC's, Network, Printer, IP cameras.
- Backup of files after every Examination.
- Maintaining LAB issue log.

Note: Lab Exam policy depends on the board requirements.

INTERNET

- Use of the Internet is for study or for school authorised/supervised activities only.
- Network resources are provided for students to conduct research and communicate with others in relation to school work.
- Use of ICT resources must not be used for personal profit.
- Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- All measures have been put in place to protect vulnerable children from inappropriate approaches and from making inappropriate personal disclosures over the school network.
- "Chat" activities are banned.
- Respect the work and ownership rights of people outside the school as well as other students or staff. This includes abiding by copyright laws.
- Games may not be downloaded or played on any School ICT equipment.
- All Internet use on ICT resources is monitored on an on-going basis.

- Students need to be aware that e-mails sent and received as part of classroom activity are subject to monitoring.
- Parents must understand that their child may encounter material that they consider inappropriate (i.e. Vulgar Jokes, statements of belief that some may consider immoral, pornography, etc.,) The student is responsible for not pursuing material that could be considered offensive.

Internet Filter

School is having **4** group SSID's (Admin, Teachers, Student and Guest) for which filtering (Content/Website/Social Media) is assigned to each group.

With respect to any of School computers with Internet access, the ICT will monitor the online activities of students and staff and employ technology protection measures during any use of such computers by students and adults. The technology protection measures utilized will block or filter Internet access to any visual depictions that are Obscene, Child pornography or Harmful to students - means any picture, image, graphic image file, or other visual depiction that lacks serious literary, artistic, political values.

Anyone violating any part of Internet policy will be redirected to Vice-Principal or Principal for further actions.

E-LEARNING

ICT department ensures smooth progress of E-learning through e-Learn, e-Teach modules, youtube, google classrooms.

SECURITY & BACKUP

In order to maintain a smooth running network, disc space available for individual users to save data is limited using network management software. This acronis management and facilitates a Weekly backup of user data, meaning that it can be recovered if accidentally deleted. The media used to backup is rotated on a weekly basis.

More space can be granted for specific projects and courses (subject to availability).
We are using Cisco Meraki to maintain the network security.

Norton antivirus is installed on every networked computer in the school and also on teacher's personal laptops that access the school network. The software updates itself daily, and constantly scans for viruses to keep the network secure.

Upon entering the school pupils and their parents/guardians are required to sign an, "Acceptable Use Agreement" for computer use and internet access at school.
Procedures can be put in place for staff to be able to block pupil's internet access at school for a period of time as a sanction for inappropriate use of the internet. In the event of this occurring.

Pupils' network access can also be blocked by IT Technician in the event of more serious network abuse with a approval by the school Principal. In the event of pupils hacking into the network or attempting to disrupt the smooth running of the network, they can be suspended at the discretion of the Principal or Deputy Principal.

All Data is stored in accordance with provision of the Data Protection:

- Students to protect work by keeping their personal passwords private. Use of someone else's personal logon/name or password is forbidden.
- To protect the ICT network, security on the computers must not be breached or settings on computers altered in any way.
- Network/Computer storage areas and USB keys may be reviewed by staff.
- Students may not examine, copy, alter, rename, or delete the files or programs of another student. System administrators may, as a requirement of system maintenance, delete files that are determined to be non-essential.

- Only relevant information and photographs of students will be used on the School and CEIST website and for promotional material.

Physical and Logical Security Access of Data Resources:

- This policy governs the physical and logical access to school all systems and applications to protect the privacy, security, and confidentiality of school systems, especially highly sensitive systems, and the responsibilities of institutional units and individuals for such systems.

Principles of the school to use all reasonable IT security control measures to:

- Protect school information resources against unauthorized access and use.
- Maintain the integrity of school data
- Ensure school data residing on any IT system is available when needed
- Comply with the appropriate federal, state and other legislative, regulatory and industry requirements.

Protecting information resources includes:

- Physical protection of information processing facilities and equipment
- Assurance that application and data integrity are maintained
- Assurance that information systems perform their critical functions correctly, in a timely manner, and under adequate controls

- Protection against unauthorized access to protected data through logical access controls
- Protection against unauthorized disclosure of information
- Assurance that systems continue to be available for reliable and critical information
- Assurance that the security and forensic needs of the school are met.

Principles of the main components of the security policy for physical and logical access:

- All systems and applications will have documented policies and procedures for:
- approving and terminating access
- obtaining and disabling temporary accounts
- consistent periodic review and assessment of all accounts for continued needs with documentation as evidence of the review
- locking accounts after a period of inactivity, with the period of time appropriate to the sensitivity of the system and associated risks
- logging configurations and review.

REMOTE ACCESS CONTROL

Remote access control will be provided, after principal approval.

What does it mean to be safe online?

Students use various devices to connect to the Internet: laptops, tablets, mobile phones etc. Online Safety is ensuring that students are protected from harm and supported to achieve the maximum benefit from new and developing technologies without risk to themselves or others.

The aim of promoting online safety is to protect a young person from the adverse consequences of access or use of Internet capable devices that includes bullying and inappropriate behaviour or exploitation.

It is the responsibility of students, parents/guardians and staff to understand the risks and acceptable use, as well as how to respond to incidents involving online safety both in and out of the school environment.

Aims of the online safety policy

- protecting and educating students and staff in their use of technology and online activities
- educating students, parents/guardians and staff about cyber-bullying, including the consequences
- informing teachers and parents/guardians about their role in protecting students at school and at home
- putting policies and procedures in place to help prevent incidents of cyber-bullying within the school community
- having effectivefl and clear measures to deal with and monitor cases of cyber-bullying

UAE LAW RELATED TO ONLINE USAGE AND SOCIAL MEDIA

- Students will be informed and repeatedly reminded about the UAE laws concerning internet usage and related use of Social Media
- Students will be reminded about minimum age requirements for opening accounts with Facebook, Instagram, Snapchat etc.

Teaching and Learning

The Internet is an essential tool in 21st century life for education, business and social interaction. St, Mary's is committed to providing students with quality Internet access as part of their learning experience in order to raise attainment standards and tie in with the vision and mission of the school in creating exciting and innovative opportunities which promote student achievement and success.

We aim to ensure that:

- students will be made aware of acceptable and unacceptable Internet use
- students will be taught, where appropriate, to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- students will be educated about the effective use of the Internet
- students will be taught how to evaluate Internet content by ICT teachers
- students will be reminded to report unpleasant Internet content to their class teacher, school counselor or Vice Principal

- the school Internet access is designed expressly for student use and includes filtering appropriate to the needs of our students
- where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites they visit
- the use of Internet-derived materials by students & staff complies with copyright law
- all students keep their Active Learn usernames and passwords securely

Introducing Online Safety to students

- Online safety advice and instructions in a format appropriate for our students, will be displayed in classrooms, corridors and discussed with students as part of their learning, where appropriate
- students will be reminded continuously and informed that school network and Internet use is monitored
- Online safety and cyberbullying training will be embedded within the ICT teaching curriculum and PSHE and Moral Education Lessons

Cyber Bullying

- will engage proactively with students in preventing cyberbullying by:
- understanding & talking about cyber-bullying & displaying appropriate information for students to have constant visual reminders in all parts of the school
- keeping policies and practices up to date with new technologies
- ensuring easy and comfortable procedures for reporting cyberbullying
- dealing with all bullying complaints and incidents following the procedures set out in the Anti-Bullying Policy
- promoting the positive use of technology
- warning students about not trusting unknown online users and teaching them what information is safe to share
- Advising students to report immediately, to their teachers, Counselor, Vice Principal the receipt of any communication that makes them feel uncomfortable, or is offensive, discriminatory, threatening or bullying in nature and not to respond to this form of communication in any way

Cyber -bullying Related Sanctions

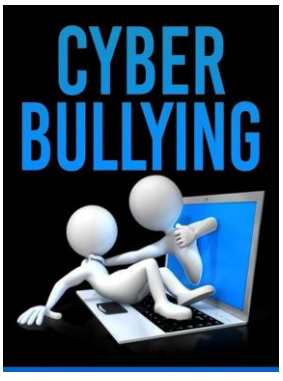
When staff/ leaders are made aware of a cyberbullying incident that involves any of our students, the Student Support Services Department & the School's Leadership Team will:

- assess the immediate threat
- ensure the safety of the student (target) by separating the bully from the target and closely monitoring the situation
- demonstrate compassion and empathy to the student
- investigate and gather evidence
- contact both student's parents
- notify key school staff
- The school will keep an evidence file of all cyber-bullying with screen shots, message logs or any other content, so that the seriousness of the behaviour and its negative impact on the school and learning environment can be demonstrated. This is vital, especially if the school intends to sanction students formally, e.g. suspensions, loss of extra-curricular privileges or inform parents.

Social networking and personal publishing

The school has a duty of care to provide a safe learning environment for all its students and staff and will ensure the following:

- blocking student access to social media sites within school boundaries
- educating students about why they must not reveal their personal details or those of others, or arrange to meet anyone from an online site
- educating both students and staff as to why they should not engage in online discussion revealing personal matters relating to any members of the school community
- educating both students and staff about ensuring all technological equipment is always password/PIN protected



Students images and work

Staff, parents/guardians and students need to be aware of the risks associated with publishing digital images on the Internet. Digital images may remain on the Internet forever and may cause harm or embarrassment to individuals.

- photographs that include children will be selected carefully
- when using digital images, teachers should inform and educate students, where appropriate, about the risks associated with taking, sharing, publishing and distributing images
- at most school events, parents/guardians are welcome to take videos and digital images but these are for personal use only
- to respect everyone's privacy, school recorded images should not be published or made publicly available on any social networking sites
- any videos or digital images taken must insure that students are appropriately dressed and are not participating in activities that might bring the individual or the school into disrepute.

ICT integration in teaching and learning for pedagogical purposes:

- Power Point Presentations
- Online Exams with assessments
- Interactive Tasks
- 'Digital stories
- Interactive Quizzes
- Videos
- Audio stories
- Simulations
- Digital puzzles
- Blogs and websites on specific topics
- Softwares
- A Multimedia projector and computer system in each classrooms (with required softwares installed)
- Computer Labs (from Primary to secondary)
- E-Learning for Teachers and students

INFORMATION SECURITY POLICY

Objective:

The objective of the policy and procedures is to define an overview of Information Security Management System for each user.

Scope:

The scope of Information Security Management System (ISMS) is the protection of Information and includes Information Management and Physical security.

1. **Security Incident Management Policy**

   The objective of this policy is to respond to and reporting security incidents/software malfunctioning, with a process for monitoring and learning from such incidents.

   Security Incident shall be defined as

   - Sensitive Information lost
   - Unauthorized access to information
   - Identity thefts
   - Misuse of computing resources and information
   - Incidents related to Physical security such as but not limited to laptop loss
   - Unavailability of service or information
   - Unauthorized Modification of Information
   - Unauthorized use of tools for monitoring, Probing, Hacking, etc.,

   Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate Security Incident Management procedures shall be followed.

   Users are made aware of procedures for reporting a Security incident.

   Security incidents shall be analyzed, and preventive/corrective actions taken to minimize recurrence of an incident.

2. **Access Control Policy**

The objective of this policy is to ensure that access controls adequately protect all of the information resources.

User Access Control:

- User access to application resources is granted on a "need to access" and "need-to-know" basis.
- Each application are maintained with access levels such as read-only, read-write, read-write-execute, etc. and the access provisioning shall be on a role-based model.
- System privileges are defined so that computer users are not permitted to update information.
- The default user access level for the files is set to no-access which blocks access by unauthorized users
- All users are identified by the unique identifier (username / password) and the access to all resources be through this id
- Users shall be held responsible for every transaction being carried out using their login account.
- Users Password shall be changed every 90 days or when requested by the user. Passwords issued by a Security Administrator will expire, forcing the user to choose another password before the next logon process is completed.
- Password shall be of minimum of 8 characters - alphanumeric characters with a minimum of 1 numeric and 1 special characters. Blank passwords are not permitted. Option to have at least 1 upper case and 1 lower case character.
- Users are advised never to store remote access information (such as fixed passwords and user-IDs) on the system.
- Responsibility of maintaining confidentiality of User Passwords shall rest with the user. Screen saver passwords shall be enabled by users on their own desktops/laptops to prevent unauthorized access.

Network Access Control:

- Users logging onto a network computer or application shall have access to the information and services required for and they have been authorized to use.
- Users shall not connect any new resources onto network without getting prior approval from IT Administrator.
- User networks have the appropriate secured Gateways/Firewall to segregate Internal and External domain and also to isolate other networks.
- Appropriate Network Routing Controls (Network segments, VLANS, etc.,) are defined for protection of CUSTOMER network from external world.
- As a standard business practice, to encourage the productive use of the Internet, IT Administrator routinely uses software (Cisco Meraki Policy) which blocks users from visiting those Internet sites which management considers being objectionable.
- Operating systems and applications are configured to run only restricted services as required.
- Systems are protected against unauthorized use by setting an activity lock out period of 5 minutes.
- If the computer system to which they are connected or which they are using contains sensitive information, users must not leave their personal computer, workstation, or terminal unattended without logging out or invoking a password-protected screen saver.
- Critical applications shall be allowed access through Internet after carrying out risk assessment and formal authorization by system administrator.
- Users are forbidden from connecting any computer to an external network, be it a private or public network, unless the advance permission of the IT administrator has first been obtained. Access to all external networks flow through firewalls.

Logging:

- All User-ID creation, deletion, and privilege change activity performed by systems administrators. All sensitive equipment's and servers are designed and implemented with appropriate means of physical and /or logical access. Use and access to removable media is controlled.

Internet & Email Usage Policy

The objective of this policy is to define acceptable usage of Internet and email services

- Users are made aware that email is vulnerable to unauthorized access and modification by third parties.
- Users access the Internet facilities at their own risk for material viewed, downloaded, or received by users through the Internet. E-mail systems may deliver unsolicited messages that contain offensive content.
- All confidential information shall be sent securely over the internet.
- All users shall use email addresses for school communication.
- Users shall not use the internet/E-mail resources for any kind of personal purposes.
- All electronic mails are scanned for malicious software.
- E-mails exchanged with other internet domains shall be subject to necessary Anti-Spam and Antivirus checks, with suitable technology controls.
- Users shall not abuse, harass, threaten or otherwise violate the legal and privacy right of others.
- Users shall not send/forward any messages containing racial or sexual slur, political and religious solicitations.
- Users shall not send/forwards any messages that is inappropriate and/or has the potential to cause harm or embarrassment.
- Users shall not use CUSTOMER internet to deliberately propagate any virus, worm, Trojan horse or trap-door program code.
- Users shall not use the resources in connection with chain emails, contests, junk email, spam emails.
- Users shall not publish, distribute or disseminate any inappropriate, profane, defamatory, infringing, obscene, indecent or unlawful material.
- Accessing pornographic sites, special interest groups, websites and personal web browsing are prohibited and suitable tools are used to prohibit the same.
- Violations of these terms governing the use of the Resources, with or without intention, will result in restriction of access to the resources & may include actions which require an investigation & appropriate disciplinary action to be taken.

Wireless LAN Policy

The objective of this policy is to define the process for secure implementation and usage of Wireless networks.

- Wireless components in all locations such as Access points, Wireless Network interface cards, etc., are registered.
- Appropriate filters for protocols are implemented between wired network and Wireless network as per the applicability in locations of implementation and nature of use of wireless networks.

- Different SSID's are created for different groups of users. (Admin, Teachers, Students, Guests)
- Log files of the Access points and other wireless devices are analyzed as per the log file monitoring procedure.
- Wireless users shall get duly authenticated to the network using access control (Like Active Directory, etc.,) after proper matching of Service Set identifiers (SSID)

Removable Media Policy

The objective of this policy is to minimize security risks and Information loss arising out of usage of Removable Media Interfaces and portable storage devices such as USB memory sticks, pen drives, entertainment devices with data storage capacities (with USB, Bluetooth and other interfaces) etc.

- Personal Removable media shall not be connected via wire or wireless connections to school assets without prior approval from System administrator.
- Users shall be held accountable for copying sensitive information in to any removable media which could cause confidentially breach causing transmission of malicious code from removable media in to school network
- Users shall be held accountable for execution of unauthorized software programs from removable media even inadvertently which could potentially lead to security incidents.
- Users shall keep their official removable devices securely to avoid any theft or unauthorized data access.

Physical Security Policy

- Equipments, information or software shall not be taken without authorized permission from the school management.
- Physical access to information systems facilities is to be restricted to authorized users only.
- Care shall be exercised to protect these areas from fire, flood, explosion, civil unrest or any other man-made disaster.
- A secured intermediate holding area (IT Room) is used for computer supplies, equipment, and other deliveries.
- Users possessing mobile devices shall adhere to mobile usage policy.
- Department managers are responsible for the disposal of surplus property no longer needed for school activities in accordance with procedures
- Parents / Guests should approach security / reception. Guest pass should be issued after screening and getting approval from the person intended to meet.

ICT CODE OF CONDUCT: Student Policy:

The use of the ICT equipment at SMCHS is a privilege, not a right. Our ICT and Internet services will be made available for all students to use solely for educational purposes. Training will be provided for their appropriate use.

All students may have access to Information Technology equipment and the Internet for the purpose of:

- Support for learning
- Email contact with other students, staff, members of administration.

Responsible Information Technology and Internet Use

The computer system is owned by the school. This Responsible Information Technology and Internet Use statement helps to protect students, staff and the school by clearly stating what use of the computer resources is acceptable and what is not.

- Irresponsible use may result in the loss of Computer/Internet access.
- School computer and Internet use must be appropriate to the student's education.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- Copyright, intellectual property rights and UAE laws must be respected.
- E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.
- Users are responsible for e-mail they send and for contacts made.
- Anonymous messages, chain letters, are not permitted.
- "Spamming", cyber bullying and the use of chat rooms is not permitted.
- Access to sites containing illegal, offensive, pornographic, racially or religiously offensive material is not allowed
- Compromising or damaging the security or stability of the network is not allowed.
- The school ICT systems may not be used for private purposes, unless the Principal or Head of Information Communication Technology has given permission for that use.
- Use for personal financial gain, gambling, political purposes or advertising.

Reviewed : **September 2025**
Next Review : **June 2026**