2020 / 2021

ICT Policy

St. Michael's College

Listowel, Co. Kerry

Reviewed	Ratified by the Board of Management	Review Date
6th April 2021	13th April 2021	13th April 2021

SECTION 1: Introduction and Rationale

1.1 Introduction

Information and Communication Technology (ICT) comprises a variety of systems that handle electronically retrievable information. These include computers, digital resources, CD/DVD players, calculators, digital cameras, overhead projectors, scanners, personal devices, visualisers, video cameras and more. ICT also involves creating, collecting, holding, processing, presenting, and communicating information in a variety of ways for a variety of purposes.

This policy provides information on ICT and its development and integration into school life at St. Michael's College. This policy relates closely to the existing Data Protection Policy and Child Protection Policy, which are available on the school website www.stmichaelscollege.ie. It should be read and referred to in conjunction with same. This policy has been developed with due regard to the recommendations of ICT Policy Unit of the Department of Education and Skills (DES).

1.2 Rationale

The management and administration teams at the College use a number of powerful ICT systems to provide accurate, live and archived data on many aspects of school life, including: enrolment, attendance, attainment, timetabling, behaviour, child protection concerns and external and internal communication.

For teaching staff, ICT is an effective tool which enhances the standard of teaching and learning in many ways. Equally importantly, ICT is used to support the administrative work and recording of information that is a significant part of the work of teachers.

Students at the College are encouraged to develop and use ICT skills in order to enhance their research skills and employability, equip them with optimal access to information and to make them ICT competent in everyday life. Students should understand that ICT is a continuously changing set of tools, which requires learning, understanding and boundaries in order to use it effectively and safely.

For all school partners, competence in the area of ICT makes more effective and efficient use of time and expertise.

SECTION 2: ICT in Management/Administration

Overall responsibility for the provision and use of ICT at St. Michael's College rests with senior management. The Principal, in consultation with staff:

- determines the ways ICT can support, enrich and extend the curriculum
- determines the provision and allocation of resources
- determines how records will be maintained
- ensures that ICT is used in a way to support the aims and objectives of the College
- ensures that there is an ICT policy in place.

At St. Michael's College, several ICT systems are used to effectively and efficiently run the day-to-day business of the school, provide management and administrative staff with records and archives of students' personal details and progress and to inform strategic planning decisions. This includes:

- MANAGEMENT INFORMATION SYSTEM (MIS): COMPASS is the main database employed to provide attendance, personal, assessment and progress data on each student and to provide timetabling structures for teaching staff;
- INTERNAL COMMUNICATION: The main electronic form of internal communication is through the @stmichaelscollege.ie Google domain;
- EXTERNAL COMMUNICATION: This is supported through the use of the Parent Text/Email/COMPASS system, the school website (www.stmichaelscollege.ie), the school Twitter, and Facebook page;
- NETWORK: A comprehensive network supports the schoolwide use of cloud and server based secure processing and storage. A secure wireless network supports the use of a large number of wireless devices throughout the school;
- WEEKLY UPDATES: A weekly 'News and Information' email provides staff with weekly updates on school life;
- CCTV CAMERAS placed strategically in school environment are utilised to protect students and staff;
- LANDLINE phone system (068 21049).

SECTION 3: ICT in Teaching and Learning

3.1 ICT is effectively used by teaching staff to enhance teaching and learning and to facilitate the effective use of time and competencies. Continuous professional development (CPD) is actively encouraged across areas of ICT which will assist teaching staff to record student progress, build exams, locate, or generate and share resources, and gain further knowledge in their subject areas, etc. Building ICT competency is guided by engagement with the Digital Strategy Framework for Post Primary Schools (https://www.education.ie/en/Schools-Colleges/Information/Information-Communications-Technology-ICT-in-Schools/digital-learning-framework-post-primary.pdf)

Integrating ICT into teaching and learning aims to achieve the following:

- extend and enhance learning across all areas of the curriculum by creating, using and adapting high quality digital teaching resources;
- contribute to raising standards in literacy, numeracy and other areas of learning;
- encourage students to select and use ICT to access a variety of sources of information and a variety of learning experiences;
- develop students' skills in the safe and responsible use of ICT in line with this policy;
- enable students to extend their learning beyond the school environment and instil in students a sense of confidence, achievement and enjoyment;
- ensure teaching staff are motivated and skilled in the use of ICT and aware of the contribution ICT can make to learning and teaching;
- meet individual student needs and abilities through differentiated teaching methodologies and facilitate access to resources particularly for students with learning difficulties;
- enhance effective group work and collaborative learning;
- provide an online content management system to support learning, e.g. Google Drive shared with students and teaching colleagues.

3.2 ICT for Additional Educational Needs (AEN)

For students with learning difficulties and/or physical or sensory disability, appropriate use of ICT can often enhance many aspects of the curriculum. Appropriate software and hardware, wherever and whenever possible, are provided to facilitate access for students with learning difficulties. This may include the following approaches:

- the school applies for assessment of students' special needs in order to obtain Assistive Technology (AT) at the earliest opportunity;
- AEN students may have access to additional resources such as laptops with specific software to support curriculum access;
- where a special needs group has a diversity of needs, teachers may source suitable materials online;
- if a student with writing difficulties needs to type examination answers, appropriate access is provided and extra time is allocated.

3.3 ICT in Teaching and Learning – Teaching Remotely and Video Conferencing Tools

The school will conduct an annual risk assessment associated with teaching remotely (available in Appendix I). It is noted in this risk assessment that best practice, for Child Protection purposes, when teaching remotely is to have student cameras / microphones switched off. However, for effective teaching and learning to take place it may be necessary to have both enabled. In these circumstances, teachers must be mindful of the risks involved and take care to adhere to the guidelines below and in the risk assessment.

General guidelines for video calling and live lessons:

- The video conference room is a classroom and the same school behaviour and codes of conduct apply to this environment;
- Ensure that the background visible for the video call is appropriate and does not contain personal aspects;
- Anything unsuitable should be removed from the background setting for both teachers and students when calls are taking place for both parties. Blurring functionality and the use of a static image are features of some of these tool;
- Teachers must turn on necessary security settings before allowing students to join the call e.g. chat feature, waiting room, etc. where applicable;
- The teacher should always invite the students to the call and act as hosts. If a co-host function is available on the chosen platform, this should be disabled for students;
- The teacher is always first in the room (deploy waiting room where possible);
- Pre-set the video meeting to mute participants' microphone automatically upon entry (if possible). You can choose to switch them on selectively to allow student participation;

- It is crucial that the teacher is always the last to leave the online meeting room to ensure that students cannot re-join the room afterwards;
- Agree protocols in advance with your students, e.g. using the chat feature for questions, raising hands if they wish to ask a question, asking students to mute microphones at the beginning of a lesson in order to improve sound quality. This list is not exhaustive and will vary depending on the tool being used and the age of students;
- Maintain a log of calls and a record of attendance as you would do in general practice;
- As students may not be able to attend live classes due to lack of devices in the home setting, teachers may instead choose to record their class/screencast a lesson and share it with students using the chosen school platform (Google Classroom) or via an email link.

SECTION 4: Provision of and Planning for ICT

General ICT skills are considered an essential tool which will better prepare students for the world of work and empower them to take responsibility for their own learning.

- Transition Year students compile an ePortfolio which is presented and assessed twice during the school year. Assignments are encouraged in electronic form. Students are encouraged to integrate their computer skills classes with a reflective learning approach. Classes vary in form: lecture presentation, demonstration and practice of skills, self-directed learning and use of virtual learning environments. Students are encouraged to track their learning and progress throughout the year, to enter local and national competitions and to interact with their teachers and outside agencies through their school email. Students explore opportunities in Enterprise, the Arts and Sciences through the use of ICT.
- ICT is planned for and delivered as an integral part of each curriculum area and is routinely on the agenda of all subject department meetings.
- The Digital Learning and School Self-Evaluation teams are responsible for the development of the Digital Learning Plan (DLP)
- Students have timetabled classes.

Staff and students have access to ICT through the school network system which consists of servers, a projector in each classroom, one computer room, and wireless access points. There is a strong culture of digital collaboration in the school. Students have access to resources shared online by their teachers.

ICT provision within the school is continuously reviewed.

SECTION 5: Internet and E-Safety

St. Michael’s College recognises the need to ensure that all students are responsible and safe users of ICT and this is supported through this Policy.

Whilst St. Michael’s College offers a safe online environment through the PDST filtered internet access, it is important to educate students about online safety and their responsibilities when using ICT. Students are made aware that any misuse of mobile phones/websites/email/apps should be reported to a member of staff immediately.

All software in use at the College is used in strict accordance with the license agreement. No personal software is permitted to be loaded onto school computers. The school’s Data Protection Policy governs all matters relating to the retaining and processing of personal data on all members of the school community.

Instances of misuse of the internet or cyber bullying of students or staff will be regarded as very serious offences and are governed by the school’s Anti-Bullying Policy, Code of Positive Behaviour, and Child Protection Policy.

SECTION 6: Monitoring & Evaluating ICT

The Digital Learning Team along with senior management is responsible for:

- facilitating the use of ICT across the curriculum in collaboration with all subject coordinators;
- providing and/or organising training to keep staff skills and knowledge up to date;
- advising colleagues about effective teaching strategies;
- developing and facilitating the rollout of the DLP including new software and hardware recommendations.

SECTION 7: Continuous Professional Development

St. Michael's College recognises the need for ongoing development of ICT capability to reflect the constantly changing nature of technology. CPD for all staff is encouraged and provided in accordance with the Designated Liaison Person (DLP). This is based on audits of identified need as well as external developments in ICT. Ongoing ICT training is promoted and facilitated both within the school structures and through external ICT agencies e.g. PDST.

SECTION 8: Legislation

The school advises that teachers, students and parents should familiarise themselves with the following legislation relating to use of the Internet and IT:

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- The Data Protection Act 1988
- European General Data Protection Regulations 2018

SECTION 9: ICT Technical Support

An external contractor (DCE Computers) is responsible for upgrading and monitoring the school's ICT facilities. The maintenance of all school ICT facilities is everyone's responsibility in the first instance. All teachers have the primary responsibility in safeguarding equipment and identifying when a problem occurs.

SECTION 10: Implementation and Review

This policy and its implementation will be reviewed by the Board of Management once in every school year. Written notification that the review has been completed will be made available to school personnel, published on the school website, and provided to the Parents Council. A record of the review and its outcome will be made available, if requested, to the Trustee and the Department.

Signed: ______________________________ Signed: ___________________________

(Chairperson of Board of Management) (Principal)

Date: ________________________________ Date: _____________________________

Date of next review: ___________________________

APPENDIX I

RISK ASSESSMENT ASSOCIATED WITH TEACHING REMOTELY

St. Michael's College 2020/2021

The National Centre for Cyber Security has published helpful guidance on working from home. It can be accessed at https://www.ncsc.gov.ie/pdfs/WFH-Advisory.pdf

	RISK	TYPES OF RISK	ADVISED ACTIONS
1.	Hard documents with personal data in the home	Files removed from the school	Keep a written record of files taken home
		Printing material	Avoid printing where possible. Store printed documents in line with their sensitivity
		Storage of documents	Ensure security & confidentiality - locked cabinet
		Disposal	Shred when no longer required
If a data breach occurs the school must be informed without delay			
2.	Staff using own devices	Accessibility of device(s) to others	Device should be password protected Device screen not visible to others when personal data being accessed Automated screen savers Care around security of external storage e.g. USB
		Cybersecurity of devices	Anti-virus software installed and up-to-date Operating system up-to-date Device firewall up-to-date Device storage encrypted 2 factor authentication activated for accounts that allow access to school data

			Default passwords changed on software and devices No storage of school data on personal devices

3.	Cybersecurity	Increase in phishing related to COVID-19	Advise staff on the nature of phishing and what to look out for
4.	Communication Channels https://www.education.ie/en/Schools-Colleges/Information/Post-Primary-School-Policies/Policies/continuity-of-guidance-counselling-guidelines-for-schools-providing-online-support-for-students.pdf	Email communication	All email communication should be via “work” rather than personal email addresses
		Use of applications and platforms	Approved applications and platforms only This school approves google suite. Voice/text/other apps only to be used in exceptional circumstances
		Online discussion of identifiable students, including special category data e.g. AEN	Keep such online discussions to a minimum Preferable to use direct telephone conversations
5.	Other GDPR issues	GDPR compliance when using systems such as Google suite	If staff use this (G Suite) platform in an appropriate and secure manner confidence in complying with GDPR is high Issue and advise staff to follow Data Protection Commission (DPC) advice on remote working (see link in section 4)

6.	Online tools and platforms	Use of appropriate platforms	Consult PDST website for list of most appropriate options Share the Computer Education Society of Ireland website with staff for advice and practical experience of others http://www.cesi.ie/cesi-mailing-list/ Discourage use of unapproved technologies - may present significant cyber security and data protection risks Ad hoc use of apps or services are discouraged Teachers should not use personal accounts/emails to access unapproved platforms
		Implementing controls and security measures within an application or platform, even those used previously in school.	Advice on data security and risk management published by platform providers (g suite) should be reviewed by staff
		Personal data breach	Sharing of personal data on online platforms to be minimised to the greatest extent possible
		Inappropriate behaviour on online platforms	Staff, students, parents reminded that all school policies, notably, Code of Positive Behaviour and Acceptable Use Policy (AUP) apply online
7.	Video or real-time teaching (National Centre for Cyber Security (NCSC) for guidance)	Online sharing of video data (teacher or students)	Keep to a minimum Focus on learning content will keep sharing of personal data to a minimum

		Recording or screenshotting data	Not allowed by students, AUP applies Serious consequences of this action should be emphasised Teachers should not record sessions unless it is strictly necessary
		Inappropriate behaviour by students Inappropriate behaviour in the background Inappropriate environment e.g. bedroom	Best practice for Child Protection purposes is to have student cameras / microphones disabled Use of student cameras / microphones should be kept to a minimum Where it is required to enable cameras and/or microphones for educational purposes students should be reminded of appropriate behaviours Suitable blurred or virtual backgrounds may be used Teachers should remain in control of settings that enable/disable cameras/microphones Minimise use of chat and file sharing functions, or disable entirely
		People other than the target group joining	Control access to the online classroom by use of a 'waiting room' function Hyperlinks, if used, not to be shared beyond the target group Enable features that alert of newly-joined participants - audible tone Use "lock meeting" function when all expected guests have joined

		Teacher home environment	Awareness of what is said/shared /overheard in the home
		Accountability and governance	School should have a written Data Processing Agreement (between school and service provider) guarantees of security measures, description of all data collected and processing activities, list of sub processors, storage location of data (with appropriate safeguards where outside the EEA), retention periods, 7 privacy policies, transparency requirements Ask service providers if they have undertaken a DPIA (Data Protection Impact Assessment) related to the use of their platform in an educational context
8.	Transparency	Lack of communication with the school community can increase the risk of data breaches	Communicate clearly with parents and students about the nature of online learning and guidelines around same