SIENA COLLEGE
CAMBERWELL
Staff Digital Technology Policy

POLICY TITLE: Staff Digital Technology Policy

DEVELOPED / REVIEWED BY

Siena College Policy Committee

REVIEW SUMMARY & RATIONALE

Digital technologies are essential tools for creation, management, retrieval and dissemination of information, and for communication. Siena College provides access to and expects all members to use digital technologies in teaching and learning and in carrying out their other roles where appropriate.

The College has a responsibility to protect the rights and safety of users, and to safeguard against misuse. Electronic communications are often public in nature and general rules and standards of ethical behaviour and use apply.

DOCUMENT DEVELOPMENT PROCESS

This document was first developed by Policy Committee member Laura McRae in 2022 based on a review and revision of the 2017 Staff Digital Technology Policy.

DEFINITIONS

digital technology:	Includes ICT, social media, online games, file and information sharing applications, messengers, multimedia, productivity applications, cloud computing and interoperable systems that store, retrieve, manipulate, transmit or receive digital resources.
digital resources:	Files or signals in a digital format that can be accessed, stored, manipulated or transmitted electronically. These may include but not limited to: data, sound, maps, animation/video, photos, sound, images, common application files like MS Excel, MS Word and Adobe PDF.
electronic communication platform :	A system for sending and receiving messages electronically over a computer network.
information communication technology (ICT):	Any technology or device that will or can store, retrieve, manipulate, transmit or receive information or digital media electronically, this includes, but is not limited to, telephones, mobile phones, computers (servers, desktops, laptops, tablets), printers, scanners, wireless or computer networks, broadcasting equipment, software, middleware, storage, audio-visual systems, electronic communication platforms , internet, intranet and extranets.
intranet:	A privately maintained computer network that can be accessed only by authorised persons, such as members of the Siena College community.
password:	A code, which, when associated with a user account, provides access to digital technology, through an authentication mechanism or a login page.

SIENA COLLEGE
CAMBERWELL
Staff Digital Technology Policy

Users:	Are College employees, contracted staff and any other persons authorised by the College accessing College digital technology.

PRINCIPLES / GUIDING PRINCIPLES

- The College's digital technology tools are to be used to assist in a manner that is consistent with the expectations of the Siena College Mission, Vision and Values
- Subject to the College's rights under this Policy, the College respects the privacy and confidentiality of users' data and restricted access is provided by means of user passwords
- Pre-service teachers and other persons may be given temporary, designated access to College digital technology at the discretion of the Principal or a delegated nominee
- Users of College digital technology must abide by relevant laws, legislation and College policies and procedures. Users are required to make use of these facilities in a manner that is ethical, legal and does not interfere with use by others
- All messages and digital resources composed, sent or received on the College's electronic communications platform are and remain the property of the College. They are not the private property of any user.
- The College reserves the right to monitor the use of the College's digital technology to the extent allowed by relevant laws and to ensure compliance with College policies. This includes remote access.
- Compliance with this policy and related procedures and guidelines, as may be updated from time to time, is a condition of employment with the College. Any breaches of this policy may result in disciplinary action which may include termination.
- Users must protect passwords at all times against disclosure or unauthorised use, including when generated, distributed, used and stored.
- Users must comply with the requirements of any College policies or guidelines relating to sed of digital technology and/or password creation, management and protection, as may be updated from time to time.

PROCEDURES

- Staff use of Digital Technology
- Email Etiquette for Siena College Staff

RESPONSIBILITY

- Principal
- Deputy Principal Learning and Teaching
- Head of IT

RELATED LEGISLATION

- Privacy Act 1988 (Cth) (including the Australian Privacy Principles)
- Copyright Act 1968 (Cth)
- Spam Act 2003 (Cth)
- Applicable Federal and State anti-discrimination legislation

RELATED SIENA COLLEGE POLICIES

- Discrimination and Harassment Free Workplace Policy 2021
- Privacy Policy 2019
- Learning and Teaching Policy 2019
- Assessment and Reporting Policy 2022
- Social Media Policy 2022
- Child Safe Policy 2016

RELATED DOCUMENTS

- Siena College Mission Statement
- Siena College Strategic Plan
- CEM Policy 2.21 Information Privacy Policy 2020

RISK

In the Committee's deliberations it is important to consider the College's main strategic processes and the identification of associated risks. Some sample questions are included for referral.
Answers are to be documented as part of the policy.

1. **Faith and Catholic Identity.** Identify any risks to Catholic Identity or Dominican charism of the school. How will this policy harm or enhance either?
2. **Reputation.** Identify if there are any reputational risks to the College. How will this policy impact Siena and wider communities?
3. **Financial.** Identify any financial risks to the College. How will this policy impact the financial stability of the College?
4. **Contemporary Learning and Teaching.** Identify any risks to learning and teaching. How will this policy impact the academic performance of the College?
5. **Wellbeing.** Identify any risks to safety and wellbeing. How will this policy impact the mental and physical wellbeing of the College community?
6. **Community Engagement**. Identify any risks to building community engagement. How will this policy impact community relationships?
7. **Governance and Leadership.** Identify any risks to governance and leadership in the College. How will this policy affect the strategic direction of the College?

Do any risks identified above warrant changes to the proposed policy? If so the policy should be referred back to the developer/s.

NEXT REVIEW

June 2025

POLICY LOCATION

Siena Central: https://sienacentral.siena.vic.edu.au/homepage/3452

SIENA COLLEGE CAMBERWELL

Staff use of Digital Technology

PURPOSE

The purpose of this document is to ensure all Siena College staff are aware of the policies and procedures for the use of digital technology provided by the College, and to be familiar with how concepts of privacy and security apply to its use.

GENERAL

The computers provided to all staff reflect the objectives of the College's policy outlined in its Mission Statement and Strategic Plan. This document clearly demonstrates the College's commitment to utilising technology to enhance learning and teaching and enable staff to work efficiently.

The software used on the computers, network and the Internet facilities provided are to be used for the delivery of the curriculum and day to day running of the College. It is important that staff be aware of their responsibilities about use and care of the College's equipment and to ensure proper utilisation of the associated technological facilities.

INTRODUCTION

Siena College has provided staff with the technological equipment and facilities to assist in achieving the College's vision. The equipment and the data stored in the system are and remain the property of Siena College. It is important that information stored on the computers relates to the purposes for which the equipment has been provided.

GUIDELINES

- It is important that care and storage of the equipment is a high priority. Should problems occur with the equipment then Head of IT must be advised immediately.
- Laptops should be stored out of sight at the end of day and where possible in a lockable cupboard.
- Time spent by staff either sending or reading private emails is permissible providing this does not require substantial expenditures of time or individual uses for profit purposes.
- Siena College reserves the right to monitor, retrieve and review the uses for which the equipment and technological facilities are utilized by each staff member.
- Staff should not assume electronic communications are totally private and confidential and should not store or transmit highly sensitive information. This especially relates to communication regarding students or their families.
- In the use of email, staff need to ensure that the guidelines set out in the Email Etiquette for Staff document are followed.
- Staff are responsible for and encouraged to save their work to the network and back up their work periodically (at least once per term). Assistance with this can be sought from the IT Services Department.

EXPECTATIONS

In using the College email and digital technology resources staff and users must not:

- subscribe and use school email address for personal purposes (social media, online shopping, travel, banking etc)
- use a password that is the same or similar to one you use on any other websites
- abuse the privilege of College facilitated access to electronic media or services.
- duplicate, distribute or alter any of the licensed software.
- use any unauthorised, unlicensed, or illegal software.
- access any computing resource or data or attempting to disrupt normal operation of any computing network.
- use another employee's computer data without their permission.
- use the College's electronic communications platforms to: falsify the identity of the source of mail messages; send

Staff use of Digital Technology

harassing, obscene or other threatening electronic mail; attempt to read, delete, copy or modify the mail of others without their permission.

- knowingly or carelessly infect any College computing resource with a software virus.
- tamper with College computer network or building wiring.
- use the College's computing network resources for personal gain or illegal activities such as theft or fraud.
- create, look up, receive or distribute pornography.
- Read or "hack" into other systems or other staff members' passwords.
- infringe the copyright or other intellectual property rights of third parties by copying, retrieving, modifying or forwarding materials except as permitted by the copyright owner.

- create and/or distribute defamatory, fraudulent, discriminatory, or harassing messages, or otherwise engage in any illegal or wrongful conduct. Download software unrelated to their employment at the College under any circumstances.
- create, look up, or distribute any material (including emails, screensavers, and internet sites) which may be offensive to another person.

PASSWORD REQUIREMENTS

- As required by the Staff Digital Technology Policy, passwords must be created and managed in accordance with the guidelines contained in Appendix 1.
- Passwords for accounts with privilege must follow stronger requirements than regular user passwords.
- Users are responsible for the safe custody of their passwords.
- Users must advise IT Helpdesk immediately if, or if you have any reason to believe, your password has been compromised.

SANCTIONS

Most sanctions will be dealt with by the Principal. The severity of the imposed sanctions will be appropriate to the violation. More serious breaches such as civil or criminal law, acts of fraud or theft will most likely result in action by the appropriate authorities.

All sanctions taken in respect of breaches of this document will be in line with the Victorian Catholic Schools and Catholic Education Offices Award and the Victorian Catholic Schools and Catholic Education Offices Agreement.

I have read and fully understand:

- the contents of this document on staff use of digital technology;
- the document 'Email Etiquette for Siena College Staff'; and
- related policies including the Staff Digital Technology Policy and Social Media Policy,

and agree to abide by all the terms set out therein.

Name.....

Signature.....Date .....

APPENDIX 1 - Password Requirements

1. PASSWORD MANAGEMENT/ PROTECTION

1.1. All access and security codes such as passwords and security tokens are considered as confidential information and must be protected and handled accordingly
1.2. Passwords must be protected at all times:
  1.2.1. Passwords must be memorised and must not be written down in plain sight.
  1.2.2. When a new user, or an existing user, requires a new password, a temporary password will be transmitted in clear text over the phone or by email when it is:
    - Randomly generated and sent out individually to each user; and
    - Valid for a unique transaction or forced to be changed after the first use.
  1.2.3. The "Remember This Password" feature in an application (typically within the web browser) must not be used unless the computer is solely used by a single user at all times (i.e. not a shared computer) and its access is protected.
1.3. Passwords used on different systems (i.e. network domain, applications, network devices, and personal passwords) or for different roles and privileges (i.e. regular user, supervisor or administrator) must each be different where possible. Specifically:
  1.3.1. The passwords used on College systems must be unique and must not be used on any other non-College systems or applications.
  1.3.2. Passwords used to authenticate to external applications, where credentials are sent over an external or public network (for example over the Internet) must be different from passwords used on the internal systems and applications.
  1.3.3. The password of user accounts with system-level privileges, such as administrator accounts, must be unique and must not be used for other non-administrator accounts.

2. MINUMUM PASSWORD REQUIREMENTS

Passwords need to meet the following complexity requirements:
2.1. Be at least 10 characters in length
2.2. Not contain your name or more than a few characters of your name.
2.3. Not contain real words identifiable with you, or your family
2.4. Contain characters from three of the following four categories:
  2.4.1. English uppercase characters (A through Z) and
  2.4.2. English lowercase characters (a through z) and
  2.4.3. Base 10 digits (0 through 9)
  2.4.4. Non-alphabetic characters (e.g. ! # $ %)

3. PASSWORD RESET

3.1. The last 5 passwords you use are remembered and cannot be re-used.

4. ADHOC PASSWORD RESET

4.1. Your password can be reset at any time.
4.2. Users can request a password reset via the IT Helpdesk

5. USER ACCOUNT LOCKED

5.1. Our system will automatically lock a user account if there are ten (10) unsuccessful log-in attempts
5.2. Users will need to contact the IT Helpdesk during normal business hours to unlock their account.

ELECTRONIC COMMUNICATIONS PLATORMS ETIQUETTE FOR SIENA COLLEGE STAFF

This document outlines the etiquette that should be adhered to when using internal and external electronic mail at Siena College. These guidelines must be read in conjunction with the *Staff use of Digital Technology Agreement* available on Siena Central (Staff Zone > Policies) and in the Siena College Staff Handbook and related Siena College policies including the Staff Digital Technology Policy and Social Media Policy.

LEGAL ISSUES

- Emails should be treated in the same manner as any other written communication such as letters, faxes or memos
- Consider the legality of what you are sending. An email message may be disclosed in litigation and may be accepted as a binding document within the courts
- Be professional and careful with what you say about others. Email is easily forwarded. Do not use email to send any message you would not want viewed by an outside party
- Keep hard copies of important emails sent and received
- You should be aware of the risks of using email for sending any confidential information
- You must not distribute downloaded copyright material of third parties via email without specific authorisation to do so. This includes software, database files, documentation, cartoons, articles, graphic files, and text

SENDER

- Do not include unnecessary people in the TO: and CC: fields. Only send an email to those who need to know
- Email messages that are not of high-level importance should not be copied to senior administration unless requested by them
- In general, if you normally address a person by his/her first name, then that is the way you should address them in an email
- Do not expect a reply from individuals included in the CC: field as the email is not directed to them

CONTENT AND FORMAT

- Include a subject heading in each email message. This should be brief and should clearly indicate what the email is about to help recipients prioritise their incoming mail
- Keep paragraphs and messages short and to the point
- When adding attachments, do not exceed 10MB
- As a courtesy, include your name at the bottom of all email messages unless there is a continuous dialogue between you and the recipient
- Capitalise words only to highlight an important point or to distinguish a title or heading. Never type the whole message in upper case as this implies you are 'shouting'
- Do not use excessive punctuation. The use of several exclamation points at the end of a sentence for added emphasis is excessive. If something is important it should be reflected in your text, not in your punctuation
- Avoid the use of abbreviations or 'trendy' spelling
- Do not sacrifice spelling for speed. Take time to run a spell checker
- Be careful when using sarcasm and humour. Without face-to-face communication your 'humour' may be viewed as criticism or harassment
- The use of email to send 'chain letters' is not permitted

SIENA COLLEGE
CAMBERWELL

ELECTRONIC COMMUNICATIONS PLATORMS ETIQUETTE FOR SIENA COLLEGE STAFF

MANAGING YOUR EMAIL

Checking Email

- Check your email regularly, at least twice a day (morning and afternoon)

Opening Email: Checking for Viruses

- You should exercise reasonable duty of care prior to opening electronic mail messages, particularly suspicious emails, to ensure that emails or attachments are virus free
- Never open attachments suspected to contain viruses or from an unknown source
- Emails suspected of containing viruses must be deleted immediately and then deleted from the *Deleted Items* folder
- Information about suspicious emails should be passed on to the Network Administrator as soon as possible
- If there is not an up-to-date virus checker on the internet connected computer, arrange with the Network Administrator to immediately install an up to date virus checker
- Only transfer files into the College's network system once these files are proven to be free of viruses

Procedure for Inappropriate Email

- You must immediately inform a member of the School Executive of the receipt of an email or attachment that breaches College policy
- A copy of the inappropriate email should be delivered personally to a member of the School Executive
- You must inform the sender of such an email to stop. An appropriate response is:
  'Please do not send me this type of material again. The contents of this email do not comply with the Siena College Digital Technology Policy. In sending me this email you are breaching the College's policies and putting me at risk of doing so. A breach of the Digital Technology Policy has serious consequences.'
- Under no circumstances should you forward emails in breach of College policy to other College users or external parties

Replying to Email

- Reply, within a reasonable time frame, to all email messages requiring a reply. When a prompt, detailed response is not possible, send a short message acknowledging receipt and giving an estimate of when a detailed response will be sent
- There is no expectation that staff respond to emails out of normal working hours
- Teaching staff are encouraged to set expectations with their students regarding replying to emails
- Teaching staff are encouraged to use the 'out of office' automatic reply function as appropriate
- Exercise care when replying to messages, especially emails sent to a group of people. Consider whether you need to reply to all, or only to the person sending the email, that is, use the 'Reply All' or 'Reply' options
- When you correspond back and forth to an email, it is often common practice to leave the entire previous messages at the bottom of the reply. This is an unnecessary use of bandwidth. When responding to a specific part of the original email, include just that section and delete the rest from your reply
- If you receive information forwarded to you by accident, you should delete the email after informing the sender that the email was received in error

Deleting Email

- Once an email has been read, it should be deleted from the mailbox. You should empty your *Deleted Items* folder regularly to remove these items completely. This ensures that the mail server is not cluttered with redundant files.

Safety Issues

- Do not divulge personal details such as home addresses, telephone numbers or other contact details via the internet, particularly if the recipient is unknown. Treat requests for such information with caution
- Do not give out login information or passwords
- Be very cautious about divulging financial information such as credit card details. Make sure you understand the risks beforehand