St Patrick's Technical College

SACE ■ TRAINING ■ APPRENTICESHIPS

Policies & Procedures 1.12

Staff Computer Network, Internet & Email

Version 6: 26 February 2014
Ratified by Board of Directors: May 2014
Review Date: May 2017

Catholic Education SOUTH AUSTRALIA

2-6 Hooke Road Edinburgh North | PO Box 65 Edinburgh North SA 5113
T 8209 3700 | **F** 8209 3777 | info@stpatstech.sa.edu.au | **stpatstech.sa.edu.au**
ABN 47 069 774 359

Version 6: 26 February 2014
Ratified by Board of Directors: May 2014
Review Date: May 2017

INTRODUCTION

The internet (including the World Wide Web) is a global network of independently managed networks. The web provides immediate access to a vast pool of global information and services, whilst facilitating timely and cost effective communication with colleagues, staff, students and the general public.

Nobody "owns" the internet and there is no single governing body that controls what happens on the internet. It does not, and was not designed, to provide the same guarantees of confidentiality and protection as conventional information systems.

With the above in mind, St Patrick's Technical College has developed a Computer Network, Internet and Email policy.

POLICY

All staff, including contractors and temporary employees, who are issued with a computer access account or have access via a St Patrick's Technical College server are to use that access in accordance with the guidelines set out in this policy.

St Patrick's Technical College staff must use the network, internet and electronic mail (email) resources in an appropriate and professional manner and in accordance with the ethical standards expected from College staff.

St Patrick's Technical College information is an important business asset and must therefore be protected to preserve its:

- Confidentiality;
- Integrity;
- Availability.

St Patrick's Technical College is committed to ensuring its information is appropriately managed in accordance with the guidelines set out in this policy.

St Patrick's Technical College is also committed to protecting and managing all assets that contribute to the security of College information. These assets include physical and environmental facilities, Information Technology and Communications equipment and application software and packages.

The access, transmission, retrieval, storage or display of the following inappropriate material:

- Sexually explicit material;
- Hate speech or offensive material;
- Material regarding illicit drugs or violence;
- Material regarding criminal skills and/or illegal activities;
- Material of a defamatory or harassing nature;

is strictly forbidden. This includes accessing any sites or forums that deal with these materials.

Non-compliance with this policy may result in disciplinary action against the employee leading to termination, refer to Policy 3.11, Disciplinary Procedures. Furthermore, any material found that may be related to child pornography or pedophilia will be referred to the South Australian police.

St Patrick's Technical College reserves the right to monitor emails and internet activity undertaken by users who have access to resources provided by the College. This will apply to situations where users access the internet or email at home or elsewhere using College equipment and/or internet services. Systematic audits of email and internet usage will be undertaken on a regular basis.

St Patrick's Technical College Information Technology and Communications equipment, facilities and information will be available during agreed operational times to authorised users.

The College recognises that, consistent with the provision of a favourable work environment and the promotion of the College as a learning institution, some personal use of computing resources is reasonable. Therefore limited personal use of email and the internet is permitted provided:

- There is no additional cost to the College;
- It does not interfere with the user's work and the activities of other employees;
- There is no effect on the efficiency of the College's network; and
- Use is not classified as inappropriate.

GUIDELINES

Network

1. Access to the service requires a password for each account. Passwords must:
    - Be at least six characters long;
    - Contain characters from three of the following four categories:
        - English uppercase (A – Z)
        - English lowercase (a – z)
        - Base 10 digits (0 through 9)
        - Non-alphabetic (for example !, #, $, %)
    - Not be a dictionary word or name (a mix of alpha and numeric characters is best);
    - Be changed regularly and when necessary; and
    - Not be written in obvious places.
2. Service level agreements are in place with equipment and service providers. These agreements provide adequate protection against excessive downtime and service interruption or degradation.
3. Problems encountered by users are to be reported to the Resource Centre Manager for referral to the network service provider for timely problem resolution. Requirements for out of hours support (other than remote access) must be negotiated with the network service provider.

4. All St Patrick's Technical College information and data is to be stored on the network file servers to facilitate file access and back-up. St Patrick's Technical College information and data must not be stored on local drives of personal computers. Staff are responsible for developing contingency procedures for applications and data stored on individual personal computers.

5. Information processing and information storage facilities are to be protected at all times from environmental threats which jeopardise the existence, functioning and availability of the information. Appropriate environmental controls for information technology equipment infrastructure include climate controls for air temperature and humidity. Other environmental factors to be considered include dust, water, vibration and electromagnetic interference.

6. Internet / Email communications attract the same laws relating to copyright and defamation as traditional publications. It is important therefore to treat the internet and any form of email in the same way as you would other published materials. Copyright material must not be copied without the copyright owner's consent.

7. Before downloading software from the internet or other storage mediums it should be scanned for viruses using up to date anti-virus software.

8. The internet is an open, non-secure data carrier. The classification and sensitivity of information communicated or published on the internet must be considered and appropriate measures taken to protect such information.

9. St Patrick's Technical College staff must comply with approved delegations in the acquisition of products over the internet. Care should be taken to only purchase from organisations that utilise appropriate security measures in their internet commerce sites.

10. Interference or disruption to other networked or shared-system users, services or equipment will not be tolerated. Interference or disruption includes, but is not limited to:

    - Distribution of unsolicited advertising or commercial electronic messages;
    - Distribution of electronic 'chain letters';
    - Distribution of offensive material;
    - Propagation of any form of malicious software (viruses, worms, etc.);
    - Use of the network to make unauthorised entry into other information systems, communications devices or resources.

11. Access to the internet is to be used primarily for St Patrick's Technical College related business purposes (e.g. communications related to College business, authorised professional development and activities related to a person's duties). Limited non-business related use of the internet is permitted. Personal usage, if subjected to public scrutiny, must not cause embarrassment or concern to the College. Unacceptable usage includes, but is not limited to:

    - Postings for non-business related reasons;

- Accessing of malicious, offensive or harassing material;
- Use for personal financial gain;
- Use of non-approved file sharing technologies;
- Use for non-business related streaming audio or video;
- Use for religious or political lobbying;
- Downloading or sharing of non-business material.

12. Downloading of shareware and unauthorised software is prohibited.

13. St Patrick's Technical College reserves the right to record and monitor internet usage for the purposes of managing system performance, monitoring compliance with policies, or as part of disciplinary or other investigations.

Social Networking

1. Staff are expected to model responsible and respectful conduct to the students with whom they work. S taff need to consider the electronic social environments they utilise as part of this community and employer expectation.

2. The internet does not provide the privacy or control assumed by many users. Staff must appreciate that no matter what protections they place around access to their personal sites their digital postings are still at risk of reaching an unintended audience and being used in ways that could complicate or threaten their employment.

3. Staff should be aware of the following expectations in considering their use of social networking sites (e.g. Facebook, Twitter, LinkedIn, etc.):

    - They have considered the information and images of them available on their sites and are confident that these represent them in a light acceptable to their role in working with students.
    - They do not have students as 'friends' on their personal/private sites.
    - Comments on their site about the College, work colleagues or students, if published, would not cause hurt or embarrassment to others, risk claims of libel, or harm the reputation of the College, their colleagues or students.
    - Use the site's authorised IT systems. Do not use personal email or websites to communicate with students

Email

1. St Patrick's Technical College's reputation as a professional organisation must not be jeoparised by improper use or conduct via email. Emails should be written using appropriate language i.e. polite and non-abusive. Usage that causes interference or disruption to other email users will not be tolerated.

2. Requests for email contents under the Freedom of Information Act must adhere to Freedom of Information procedures. Other requests for email contents must be referred to the mailbox owner's manager.

3. Staff must add a disclaimer to emails where their expressed views are not necessarily those of the College.

4. Consistent with the Spam Act, commercial electronic messages must:

   - Only be sent with the addressee's consent;
   - Clearly identify who is responsible for sending the message; and
   - Allow people to opt-out from receiving future messages.

5. Numerous websites and online services ask you to provide your email address for various purposes. Be aware that doing so may result in you receiving unwanted email, sometimes in large quantities.

6. Where a person is away for any length of time, email should be forwarded to a delegate, or alternative action taken.

Security

1. All computing assets managed by St Patrick's Technical College are protected against unauthorised use, disclosure, modification or destruction, whether accidental or intentional. Only authorised users are permitted access to St Patrick's Technical College information.

2. All access to St Patrick's Technical College information is controlled and is subject to regular auditing and monitoring. All users of St Patrick's Technical College computing assets must be authenticated before access is granted to any St Patrick's Technical College computer asset or information. The entire computing architecture of St Patrick's Technical College is protected from unauthorised external or internal use.

3. Only authorised users are permitted to use remote access processes to gain access to St Patrick's Technical College computer assets and information.

4. St Patrick's Technical College management will ensure that IT security awareness is part of staff induction and ongoing training processes.

5. All St Patrick's Technical College computing assets, hardware and software, is protected from computer viruses. Only St Patrick's Technical College approved anti-virus software is permitted to be installed on the computing assets of the College.

6. Any documents or output of confidential information that is no longer required must be disposed of in a secure manner by using a security bin or shredder.

7. It is not permitted to move computer assets from any office without proper authorisation from the Business Manager. The Business Manager must ensure that the asset register is modified to reflect the assets new location.

8. All programs and third party products (software) stored or running on St Patrick's Technical College computer assets must not be changed without written authorisation from the copyright owner.

9. Computer assets must not be left unattended in an unsecured state when working with or access is available to data classified as confidential data.

10. All security violations must be reported immediately to the user's immediate supervisor who must refer them to the Principal.

11. If a password has become known by others it must be changed immediately and reported to the Resource Centre Manager who will notify the network service provider as soon as possible.

12. Sharing of passwords or user ID's must only be permitted with the written authorisation of the Principal. All users will be accountable for any actions undertaken by their user ID.

13. All users of St Patrick's Technical College computer assets must not circulate or disclose information classified as confidential to anyone who does not have the proper authority or the right of access.

14. All users of St Patrick's Technical College computer assets must not disclose their user ID's, passwords or hand held authentication device to any other user.

15. Violation of this policy, depending on severity and nature, may result in reprimand, loss of internet and / or email privileges or termination of employment.

RELATED POLICIES

- *1.4 – Staff Code of Conduct*
- *1.5 – Sexual Harassment*
- *1.9 – Security*
- *5.12 – Student Computer Usage*
- *Staff Guide to IT Facilities*