Policies & Procedures

Information and Communication Technology and Social Media

Policy Number:ICTSM01

Ratified: June 2014

Review: June 2017

Contact Person: HR Manager

St Peter's Woodlands Grammar School
A Co-educational Anglican Primary School
ABN 93 863 669 897

Introduction

Information and Communication Technology (hereinafter referred to as ICT) and Social Media are valuable tools for aiding communication, collaboration and enhancing teaching and learning. SPW seeks to promote the safe and effective use of ICT and Social Media in the School and wider community to provide students with the skills for living and working in a changing technological and information based society. SPW also will maintain a positive presence in Social Media, promoting the School and engaging with the School Community.

Definitions

ICT

ICT includes the systematic application of computing, telecommunications (including but not limited to email, telephone and facsimile services), internet, media and other digital technologies to the collection, processing, transformation, organisation, storage, transfer, and presentation of information in all its forms, in order to enhance the performance of individuals in all School activities.

Social Media

Social Media (sometimes referred to as 'social networking') are online services and tools used for publishing, sharing and discussing information. The list of social media types is extensive with new and innovative social media sites being developed almost every day. Staff can determine what social media platform adds value to their particular need, in conjunction with the ICT Coordinator. This list is provided as a guide to the types of social media currently available:

- *Social networking sites*: are websites that allow you to create a personal profile about yourself and then chat and share information with others such as family and friends eg, Facebook, Edmodo, Myspace, LinkedIn
- *Video, audio and photo sharing websites*: are sites that allow you to upload and share videos, sounds and photos which can be viewed/heard by web users the world over eg, Flickr, YouTube, iTunes, Vimeo, SoundCloud
- *Blog*: A Blog (short for web log) is an online diary, where you regularly post about your life, your passions, business, news or other interests. It is a way of having your own space in the virtual world e.g. WordPress, Blogger
- *Microblogging apps*: are websites that post micro-blog like posts to announce what you are currently doing or engage in conversation around particular interests e.g. Twitter, Yammer, Tumblr
- *Location based apps*: (also known as Geolocation) are applications with the capability to detect and record where you and other people are located e.g. Foursquare
- *Wikis*: are collaborative websites where users create, edit and share information about a particular subject or topic e.g. Wikipedia, Wikispaces
- *Online gaming*: are games played over some form of computer network and are often based around a community of users e.g. Steam
- *News aggregation*: news aggregators provide a list of the latest news stories published by users from a range of different web sites e.g. Digg
- *Forums or message boards*: are online discussion sites where people can hold conversations in the form of posted messages e.g. Pinterest
- *Online multiplayer gaming platforms*: are multiplayer video games which are capable of supporting hundreds or thousands of players simultaneously and usually feature at least one persistent world e.g. World of Warcraft

St Peter's Woodlands Grammar School's ICT and social media facilities

All equipment and materials, software, services, data and dedicated building space used in connection with ICT, which are owned by, leased by or used under license to the School; or owned by, leased by or used under license to other bodies and which are available for use through an agreement or agreements with the School; or wherever situated where access is by means of School ICT facilities.

User

Any authorised person using the ICT and/or social media facilities. Such persons include:

- All staff members.

- Any affiliated users, whose identity may be determined from time to time by the Principal or his/her delegate.

Administrator (Business Manager)
The person appointed by the School as having delegated responsibility from the Principal for the security and management of all or part of St Peter's Woodlands Grammar School's ICT facilities.

Authorised Usage of ICT and social media facilities
- For staff members, authorised usage is usage which is lawful and which is related to teaching, educational, research, preparation, administration and information technology support activities or other agreed School related work, and reasonable personal usage, subject always to the conditions set out within this Policy.
- For affiliated users, authorised usage is usage, which is lawful and which is defined by the terms of the agreement between the affiliated user and the School.

Scope

This policy applies to all staff, volunteers and contractors working within, or for, SPW during work hours or outside of work hours on School or personal computers or other electronic communication technologies. It has been developed to assist staff members use ICT and social media to:

- Enhance the performance of individuals in all School activities through the collection, processing, transformation, organisation, storage, transfer, and presentation of information in all its forms.
- Engage internally with staff or with the wider community as a communications tool.
- Design and showcase student's work.
- Integrate with, and facilitate, teaching and learning.
- Administer social media platforms in an authorised capacity, or, make contributions in a professional or personal capacity on education-related issues.

Principles – be professional, responsible and respectful

- You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the School and your personal interests.
- You must not engage in activities involving ICT and/or social media which might place the School or any members of the SPW school community at risk, cause them embarrassment or damage their reputation.
- Reasonable personal use by staff members of these ICT facilities is permitted to the extent that it does not interfere with the duties and functions of such staff members, nor any other person or organisation.

Roles and Responsibilities

The Role of the School

SPW strives to be a best practice school in ICT and social media. SPW will provide the necessary support for this policy in terms of ongoing, adequate and appropriate professional development, human and physical resources, infrastructure and adequate funding. SPW will promote and support improving student skills, knowledge, attitude and understanding, through the integration of learning technologies into the Primary Years Program (PYP). In addition, SPW will comply with legal requirements and support classroom programs through its planning and procedures.

The Role of Parents

Parents and guardians are also responsible for setting supervision and access standards that their children should follow when using media and information sources in accordance with current legislation requirements and school policy and procedures.

The Role of Students

Students are responsible for appropriate use of ICT and engagement in social media, in compliance with specific Acts and school procedures. Communications on the information networks are public

and general school rules for student behaviour, conduct and standards will apply. Individual users of the school computer networks are responsible for their behaviour and communications over those networks. Students will comply with school standards and abide by the Student Acceptable Use Agreement they have signed.

Executive Leadership will support all staff by:

- Administering appropriate policies and procedures.
- Coordinating the availability of support materials and tools to support staff in their use of ICT and social media.
- Developing and maintaining appropriate standards, guidelines and tools for ICT and social media usage.
- Ensuring the ICT requirements for establishing social media activities and profiles are in place.
- Broadly consulting with the community to be affected by ICT and social media before establishing new media use.
- Ensuring cyber-safety user agreements are in place for all staff, children and students.
- Ensuring that staff understand and comply with this policy.
- Providing relevant training to all staff and young people who will be using ICT and social media.
- Ensuring protective practices are in place to safeguard all staff and students.
- Providing opportunities for staff and students to identify and report offensive online material or behaviour.
- Acting quickly to remedy issues when they arise and supporting staff and young people through these processes.
- Modelling best practice ICT and social media usage.
- Ensuring that ICT access has appropriate safeguards in place to protect students.
- Maintaining and publishing content to the official SPW social media accounts.
- Ensuring the appropriate management and monitoring of SPW social media platforms occurs.
- Determining the suitability of any personal usage of SPW ICT facilities.

Staff members will:

- Integrate ICT throughout the curriculum and provide guidance, supervision and instructions to students in the appropriate and effective use of such resources.
- Facilitate student access to curriculum information resources and social media appropriate to the individual student instructional needs, learning styles, abilities and developmental levels.
- Comply with school standards and abide by the Information and Communication Technology and Social Media Policy.
- Ensure approval has been granted for social media activity from the relevant member of the Executive Leadership Team.
- Teach topics contained in *Keeping safe child protection curriculum.*
- Teach strategies to maintain a positive online presence and protect identity.
- Teach children and students how to identify and avoid inappropriate materials.
- Ensure any site representing SPW conforms with SPW branding standards.

Professional use of ICT and Social Media:

When using ICT and/or posting to an official and/or approved SPW social media platform, staff and users must:

- Remain polite and respectful of the feelings and beliefs of others in all dealings on the Internet and through email and should not knowingly, or recklessly, make statements that may defame, slander a person or lower the reputation of any persons, entity or their goods or services.
- Have due regard to the rights of others to use ICT facilities in accordance with this Policy
- Not behave in a manner which unduly inconveniences other people or which causes, or is likely to cause, damage to the School's facilities, materials, equipment or reputation.
- Not behave in an abusive or offensive or harassing manner in any way, nor use the ICT facilities or social media in ways which breach the law or which may cause loss, injury or damage to any person. Inappropriate activities which may result in a breach of this Policy, include, but may not be limited to, the following:

    - Sexually harassing, racist or other discriminatory communications (either between staff at the School or to third parties outside of the School)
    - Defamatory email or messaging
    - Breaches of third party intellectual property rights due to the downloading of copyrighted material from the Internet
    - Possession of prohibited pornographic or offensive material if the School's ICT facilities and/or social media tools have been used to download, store or exchange such material
    - Breaches of a Court Suppression order
- Not attempt to interfere with the operation of the School's ICT facilities. This includes the removal of any equipment from the School without explicit permission from the Administrator. Permission is automatically granted to remove users' own printouts, files, disks, CDs and other belongings.
- Not install software on any School ICT facilities without prior authorisation of the Administrator and unless the installation is designated as part of their authorised work.
- Accept that misuse of any networks or ICT facilities at other sites where access is by means of the School's ICT facilities will be treated as misuse of ICT facilities at the School.
- Not access any data in the ICT facilities unless that data belongs to them or has been specifically and intentionally designated for public use or for the use of a group to which they belong.
- Upon becoming aware they have inadvertently obtained any data to which they are not entitled or becoming aware of a breach of security pertaining to data from any ICT facility, should immediately report this to the Administrator.
- Not, under any circumstance, in messages or otherwise, represent themselves as someone else, fictional or real, without providing their real identity or username.
- Be aware of the specific media channels and etiquette and understand the views and feelings of the target community.
- Ensure that all content published is accurate and not misleading.
- Ensure all information posted or comments made on School policy is appropriate to the individual's area of expertise and authority, remains politically neutral and does not breach any confidentiality guidelines and that a person is not the first to make a significant announcement (unless specifically given permission to do so).
- Respect copyright laws and attributing work to the original source wherever possible.
- Protect personal details.
- Use SPW branding in accordance with the SPW Style Guide.
- Ensure young people involved understand the rules of operation of each social media site, and measures are in place to protect them from any potential risks.
- Ensure that colleagues are not discussed, identified or used in photographs without their consent.
- Ensure that students' names, images and details are only used in accordance with parental permissions provided.

Personal use of Social Media:

- Staff members, volunteers and contractors must not identify themselves as employees of SPW or service providers for the School in their personal webspace unless approved by the School's Executive Leadership Team. An example where approval may be granted is for the purposes of LinkedIn. This is to prevent information on these sites from being linked with the School and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.
- Staff members must not have contact through any personal social medium with any current SPW student unless the students are family members. Contact through personal social mediums with ex SPW students, unless they are family members, is strongly discouraged.
- SPW does not expect staff members to discontinue contact with their family members via personal social media once the School starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way.
- Staff members must not have contact with student's family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.
- If staff members wish to communicate with students through social media sites or to enable students to keep in touch with one another, they can only do so with the approval of the

School and through official sites that have been approved by the Executive Leadership Team.

- Staff members must decline 'friend requests' from students they receive in their personal social media accounts. Instead, if they receive such requests from students who are not family members, they must discuss these in general terms in class.
- On leaving SPW's service, staff members, volunteers and contractors must not contact SPW's students by means of personal social media sites. Similarly, staff members must not contact students from their former Schools by means of personal social media.
- Information staff members have access to as part of their employment, including personal information about pupils and their family members, colleagues and other parties and School and School Council information must not be discussed on their personal webspace.
- Photographs, videos or any other types of image of pupils and their families or images depicting staff members wearing School uniforms or clothing with School logos or images identifying School premises must not be published on personal webspace.
- School email addresses or other official contact details must not be used for setting up personal social media accounts or to communicate through such media.
- Staff members must not edit open access online encyclopedias such as Wikipedia in a personal capacity at work. This is because the source of correction will be recorded as the School's IP address and the intervention will, therefore, appear as if it comes from the School itself.
- SPW logos or branding must not be used or published on personal webspaces.
- Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the workplace.
- Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

Copyright and Software Licensing

- Users must not use the School's ICT facilities to infringe the copyright of any person. Users must be aware of the law of copyright as it affects ICT software. Software must not be used, downloaded or copied except with the express permission of the copyright owner.
- Software used on the School's ICT facilities may be subject to the Copyright Act, 1968 (Commonwealth) and therefore usage may be subject to conditions.
- Users are personally responsible for complying with the Copyright Act relating to the use of ICT software and to the terms and conditions of the particular contract or software license relating to each item of leased or purchased software.
- The Copyright Act makes specific provision for the making of a backup copy of either the original or an adaptation of an ICT program. This reproduction can be made only for the purpose of being used in the event that the original copy is lost, destroyed or rendered unusable. Such a backup copy cannot be made from an infringing copy of the software or where the copy of the software or where the copyright owner has given express directions to the contrary.
- Other than for authorised backup copying, the reproduction of ICT software constitutes a breach of the Copyright Act and may result in legal action against the offender.

Disclaimer

St Peter's Woodlands Grammar School Inc. accepts no responsibility for any damage or loss arising directly or indirectly from the use of any ICT facilities or for any consequential loss or damage. The School makes no warranty, expressed or implied, regarding the facilities offered or their fitness for any particular purpose.

The School will not be responsible for the loss of any data or software stored in the ICT facilities. Although standard back-up procedures may be in operation on some ICT facilities, the user is responsible for the maintenance of copies of any data or software controlled by the user.

While reasonable care, consistent with good business practice is taken, the School does not guarantee the confidentiality of any data stored on any School ICT system or transmitted through any network. For the purpose of managing the ICT facilities, it may be necessary to monitor files and usage. The School reserves the right to examine or copy files or data on School ICT facilities to maintain a secure, efficient and effective ICT environment and to ensure compliance with this Policy. In any cases user files will be copied to provide back-up for disaster recovery and network traffic will be sampled to ensure correct functioning of equipment.

Breaches of the Policy

Alleged Breach

Where an alleged breach of this Policy has been brought to the attention of the Administrator, the Administrator must:
a) Act to prevent any continuation of the alleged breach of this Policy pending investigation;
b) Advise the person of this Policy and require the person to discontinue immediately the alleged breach;
c) Promptly notify other relevant authorities, including the Principal of the School.

Investigation

a) The Principal or nominee will conduct an investigation of the alleged breach within 7 working days of being notified of the alleged breach of this Policy:
b) If, as a result of the investigation, it is concluded that no breach of this policy has occurred, no further action will be taken against the person, and no record of the investigation will be placed in that person's file;
c) If, as a result of the investigation the Principal concludes that a breach of this Policy has occurred, then appropriate disciplinary steps will be taken by the Principal in relation to the staff member concerned.

Breach of this policy may result in disciplinary action being taken against the staff member. Disciplinary action may include limitation or removal of access to School Systems or termination of employment or a volunteer's or contractor's engagement with SPW.

If staff notice inappropriate or unlawful online content relating to the School, or content published in breach of this policy, this should be reported to the Principal or relevant member of the Executive Leadership Team.

Review Process

A policy review to take place on a three-yearly basis.

Further information

Further information regarding this policy is available from the Executive Leadership Team and the ICT Coordinator

Related Policies

- Behaviour Management
- Bullying and Harassment
- Communication
- Information Communication Technology Rules for use of internet and email
- Privacy
- Grievance Procedures for Parents
- Volunteers
- Staff Procedural Manual

Related Forms

Student Acceptable Use Agreement

Related Documents

SPW Social Media Strategy