ACCEPTABLE USE OF ICT AND SOCIAL MEDIA

Document No:	012 of 2019
Document Type:	Policy
Publication Date:	2 July 2019
Replaces Document & No:	Responsible Use of ICT and Social Media Procedures (101101) Responsible Use of ICT and Social Media – Staff Guidelines (101200)
Author Service Area:	People and Culture
Review Date:	July 2022

Catholic Education
Diocese of Parramatta

CATHOLIC EDUCATION, DIOCESE OF PARRAMATTA

ACCEPTABLE USE OF ICT AND SOCIAL MEDIA

1. INTRODUCTION AND PURPOSE

This document details the appropriate use of information and communications technologies (ICT) and social media.

ICT include computers, mobile phones, PDAs, iPads, email, internet and network services, portable data storage devices, online data storage mediums, telephones, printers, fax machines and all other digital communications devices.

Social media means web-based and mobile technologies which turn communication into interactive dialogue. Examples include but are not limited to Facebook, Snapchat, Instagram, YouTube, Twitter, blog or wiki posts and comments.

2. SCOPE

This document applies to all staff members of CEDP. It informs staff members of their obligations and responsibilities when using ICT and social media for work-related purposes and, in limited circumstances, personal purposes. It also seeks to minimise threats to CEDP's information security and systems.

Staff members include paid employees, religious, volunteers, contractors, sub-contractors, consultants and students on work placements who use ICT for the purpose of work within CEDP.

A breach of this document may result in reduced or withdrawn access to ICT and social media and/or disciplinary action, including termination of employment. It may also result in notification to an external agency e.g. the NSW Police, if the conduct also constitutes a criminal offence.

3. PRINCIPLES AND RESPONSIBILITIES

CEDP's ICT are provided to staff members for business purposes so that they may perform the duties of their position and fulfill the CEDP strategic intent.

Staff members have a responsibility to be productive during their working hours and to be efficient, ethical and lawful in their use of CEDP's ICT and social media. Conduct that is considered inappropriate in the workplace is also inappropriate in electronic forms of communication. The use of CEDP's ICT and social media must be consistent with CEDP's *Code of Conduct* and *Code of Conduct When Working with Children and Students, Privacy Policy* and *Privacy Compliance Manual.*

When communicating through ICT or social media for work-related purposes, staff members should remember that sending such communication is similar to sending a letter on behalf of CEDP. Therefore such communication is to be courteous, respectful and expressed in a clear and professional manner.

4. **INAPPROPRIATE** USE OF COMMUNICATION SYSTEMS AND DEVICES

Each staff member has a responsibility not to engage in conduct which could impact on the safety and wellbeing or damage the relationship between CEDP and students, staff members, clients, customers, or members of the community; or that could damage CEDP's reputation or standing in the community or cause embarrassment to CEDP.

Staff members must not seek out, access, create or send material that may be considered offensive, obscene, pornographic or illegal (for example accessing child pornography). Allegations of illegal use of ICT or social media will be notified to the NSW Police.

Staff members must not mislead, abuse, vilify, victimise, defame, harass, bully, threaten, intimidate or discriminate others though ICT or social media. Staff members may also be found individually liable if they assist others through ICT or social media to discriminate, harass, victimise or vilify colleagues or any members of the public.

Staff members must not use ICT or social media in such a way that breaches the privacy of others (see the CEDP *Privacy Policy and Privacy Compliance Manual* for further information).

Staff members must not engage in inappropriate contact with students via ICT or social media. Staff members must not capture or use digital records (images, videos, audio recordings) of students other than for approved educational purposes.

Staff members must not infringe copyright or other intellectual property rights when distributing information over the CEDP network. Staff members who are unsure whether they have authorisation to distribute information should link to and attribute the source, rather than copying from it. Most software, apps and online tools have associated licensing terms and conditions. Staff members must comply with these before installing or using these tools.

Staff members must not spam, forward chain or junk mail or transmit offensive jokes.

Staff members must not deny access to other authorised users, grant access to unauthorised users or obtain access to privileges without authorisation

Staff members must only access chat rooms, download video files or downstream from the internet using CEDP's ICT or social media for genuine work-related purposes.

If a genuine work-related reason exists that requires a staff member to access sites, material, or download data that would normally be considered inappropriate, approval is required by the relevant manager prior to accessing the information and the information should be accessed in a private and secure location, and a record kept of the access.

5. **PERSONAL USE OF CEDP'S ICT**

CEDP permits personal use of its ICT by staff members where it is kept to a minimum and/or does not interfere with the effective and efficient performance of duties. Personal use of CEDP's ICT is subject to the same terms and conditions set out in this document.

The use of CEDP's ICT for personal use is a privilege which can be revoked by CEDP at any time, including where it has been used for inappropriate purposes or where the personal usage is excessive. Excessive personal use includes spending long periods of time using CEDP's ICT, downloading large volumes of data unrelated to work and live streaming.

Staff members need to remember that any information stored or processed through CEDP's ICT is the property of CEDP.

In any personal communication using CEDP's IT network, staff members should identify themselves as an employee of CEDP and include a disclaimer making it clear that they are not speaking on behalf of CEDP, that the views expressed are those of the author only, and they do not represent the views of CEDP.

6. MONITORING

CEDP will regularly monitor and may copy, access or disclose any information or files stored, processed or transmitted on its ICT, including internal or external communications, documents stored on the network, internet usage, duration and sites visited. This includes monitoring the employer's systems and devices outside of regular business hours and personal communications where they were communicated through CEDP's ICT. There may be occasions where a third party may undertake this monitoring on CEDP's behalf.

Staff members who use CEDP's ICT for personal purposes must not consider this information to be private as they will not have the same personal privacy rights as they would if they were using private communication systems or devices.

CEDP reserves the right to remove any inappropriate material from its ICT without notice.

7. USE OF PERSONALLY OWNED ICT

When using personally owned devices for work-related purposes staff members must obtain technical assistance to ensure that the device is CEDP network compliant. The terms and conditions outlined in this document apply when using personal devices for work-related purposes.

8. SOCIAL MEDIA

The terms and conditions outlined in this document apply to staff members accessing and using social media platforms for work-related purposes and for personal purposes where it is connected to or impacts a staff member's employment with CEDP.

8.1 Work-related Purposes

Social media can be used to achieve positive educational experiences. Staff members can use social media to connect with students and other professionals as long as they are interacting professionally in support of the CEDP strategic intent.

Students under the age of 13 must not be allowed to access social media platforms. Age restrictions for social media sites must be followed. Where social media is used for educational instruction for students above age 13, these are to be accessed under appropriate supervision.

Separate identities should be maintained for a staff member's professional and personal use of social media.

Staff members must ensure that any references to CEDP are accurate and do not breach confidentiality requirements.

Staff members must be expressly authorised by CEDP to use social media platforms to make comments on behalf of the organisation. CEDP reserves the right to request certain subjects be avoided, decline to use certain social media platforms and remove inappropriate comments from them.

Where authorised by CEDP to access and use social media on behalf of the organisation, staff members must ensure that any information submitted to social media platforms is in accordance with the authorised parameters, and that they only post comments that fall within their area of responsibility.

8.2 Personal Purposes

Whether staff members are using their own ICT or that of their employer, they must exercise caution when using social media platforms for personal purposes to ensure such usage will not damage the relationship between the staff member and CEDP; or damage CEDP's interests in any capacity or be incompatible with the staff member's duties as an employee. Where this occurs, the staff member may be subject to disciplinary action, including termination of employment. Conduct that could damage the relationship includes but is not limited to, derogatory, offensive or discriminatory statements or comments about supervisors, other staff members or CEDP generally.

Staff members must not invite children or students with whom they come into contact as part of their engagement with CEDP to join their personal electronic social networking site/s or messaging sites/apps or accept children or student's invitations to join theirs.

---

9. SECURITY AND PRIVACY

All ICT can be subject to hacking, tracing, phishing and interception. To assist in safeguarding the organisation against this, all staff members will be assigned a username and password. These details must be kept confidential and not be disclosed to anyone unless there are exceptional circumstances and approval has been given by the appropriate manager. Staff members must not allow another person to use their username or password as they may be held responsible for the other person's actions. They must also not use another person's username or password.

Staff members must exercise caution when opening an email from an unknown source, particularly if the email requests information regarding passwords or other personal information.

In the course of carrying out work-related duties, staff members may have access to, or handle personal information relating to others. The *Privacy Act 1988* requires staff members and CEDP to take reasonable steps to protect personal information from misuse and unauthorised access. (See the CEDP *Privacy Policy* and *Privacy Compliance Manual* for further information). It is therefore critical that staff

members take responsibility for the security of their personal devices and not allow them to be used by an unauthorised party, including anyone who is not an employee of CEDP. To assist in this, staff members should lock their screen or log out when they leave their devices unattended.

Staff members must ensure that their email address contains the CEDP's standard email disclaimer which is set to appear automatically on each outgoing email.

It is also recommended that staff members use the blind copy option when sending emails to multiple recipients where disclosure of email addresses impinges upon the privacy of the recipients. Staff members should also be aware of confidentiality and privacy concerns when speaking on mobile phones about work-related issues in public places.

---

10. FURTHER INFORMATION

Further information about this document can be sought from People and Culture by on 9840 5620 or enterpriseservicedesk@parra.catholic.edu.au .
