GUIDELINES

Responsible Use of ICT and Social Media - Staff

Number
101200

Implementation date
1 March 2012

Service area
Strategic Accountabilities

Location
CEDP

Head policy
Communications Policy
(in progress)

Catholic Education
Diocese of Parramatta

ICT, social media, and the promotion of learning in a digital world lead to challenges for educators and those involved in education. These guidelines outline best-practice advice on their use in a way that promotes learning. These guidelines apply to all CEDP staff, contractors and volunteers.

1. Ownership

CEO, as the employer and as owner of the network, is the owner of ICT provided to staff. They are work tools intended to be used primarily for business and educational purposes. CEO is the owner of copyright in all works, including electronic communications such email messages, documents, images, video and audio files, and other internet content created by its staff in the course of employment.

2. Monitoring

CEDP respects your privacy but be aware that your use of ICT is subject to supervision and monitoring.

CEDP provides a standard operating environment for all desktop and laptop devices. These devices, by default, have the ability to allow remote monitoring to support the user by allowing helpdesk to assist with trouble shooting. The user enables this remote access request to their device by accepting the connection request.

CEDP does not store or maintain log files of individual usage on any device. No Spyware or malicious software is installed.

CEDP does, however, monitor internet usage to ensure that no inappropriate sites are accessed on our network.

System administrators and limited authorised personnel may monitor and audit contents and usage of ICT. There may be occasions when a third party may monitor email, internet or network usage on CEO's behalf. This may include emails which are sent to or by you. This includes the sites and content that you visit, the length of time that you spend using the internet. You should be aware that this monitoring may occur both during and outside business hours. CEDP may copy, access or disclose any information or files that are stored, processed or transmitted using the CEDP network. You should structure your content with recognition that it is not private as all information on the CEDP network will be treated as education or business related content. CEDP may block access to certain websites and delivery of certain messages.

Emails may be archived as CEDP system administration considers appropriate. Backups and archives may also contain copies of emails that have been deleted by the user.

3. Personal use

You are permitted to use ICT to send and receive personal messages, if such use is kept to a minimum and does not interfere with the performance of your work. You should be aware that any use of CEDP network or email for personal purposes is subject to these guidelines. Inappropriate or excessive personal use of ICT during work hours may lead to disciplinary action.

In the case of shared ICT you are expected to respect the needs of your colleagues and use these in a collaborative manner to support student and professional learning.

4. Personally-owned devices using CEDP network

When using personally owned devices for employment purposes:

- obtain technical assistance from ICT to ensure that the device is CEDP network compliant
- be aware that their use is subject to these guidelines.

5. Content

All digital communications should be treated as a permanent written record which may be read by persons other than the intended audience and which could result in CEDP's liability.

What you create digitally (in email, text messages, comments, social media, on websites or servers) is potentially neither private nor secret. It may be easily copied, forwarded, saved, intercepted, archived and may be subject to discovery and litigation. Inappropriate content may be seen by many people you would not expect and is not easy to erase.

Content that may seem harmless to you may seem highly offensive to someone else. You should be aware that, in determining whether digital content is inappropriate supervisors may consider the responses and sensitivities of both your intended recipient of the content and any other person who may access the content.

Comments that are not appropriate in the workplace or school environment will also be inappropriate when sent made using ICT or social media. Digital communications can be easily misunderstood so you should express yourself in a clear professional manner.

Be particularly careful of 'chain-mail' emails which are apparently amusing or interesting and which are forwarded to you with the invitation to forward further: This is one of the commonest ways in which viruses are spread.

If you receive inappropriate digital content you should delete it immediately and not forward it to anyone else. It may be appropriate for you to discourage the sender from sending further material of that nature and to discuss the most appropriate action with your supervisor.

6. Some important 'Dos and Don'ts'

All staff may use ICT and the CEDP network to:

- act professionally in accordance with your role
- join educational or role specific professional groups
- have a professional profile in keeping with your role.

You should never use ICT and the CEDP network to:

- access violent, pornographic, obscene, horror or hate inciting sites
- deny access to other authorised users
- grant access to unauthorised users
- obtain access to privileges without authorisation
- inspect, modify, distribute or copy proprietary data, directories, programs, files or software without authorisation
- circumvent security settings of CEDP ICTs
- belittle, abuse, vilify, defame, bully, harass, discriminate (by virtue of sex, race religion, national origin or other)
- injure the reputation of CEDP or in a manner that may cause embarrassment to CEDP
- spam or mass mail
- give away or discuss CEDP's confidential information
- do anything that could be viewed as derogatory towards, or disparaging of, colleagues, parents or students; or undermines their effectiveness at work (eg. through excessive use)
- capture digital records (images, videos, audio recordings) of students which may be inappropriate
or for unlawful purposes.

7. Some social media 'Dos and Don'ts'

Keep your professional and personal life distinct! The easiest way to do this is to have separate identities for your professional and personal use of social media such as Facebook, Twitter and YouTube. Ask yourself: how would a member of the public view my communications or my professionalism? If uncertain discuss with your supervisor and ask for advice.

Social media are powerful tools for achieving positive educational experiences for our learning community. As long as you are interacting professionally in support of the CEDP strategic intent, you should use Facebook, WikiSpaces, Twitter, Youtube and similar media to connect with students and other professionals.

DO use social networking tools to:

- be professionally accessible to students
- share presentations and notes with students
- answer questions from students - within hours negotiated with students and supervisors
- share photos or videos of your students' work - with their knowledge and consent
- find other teachers to exchange ideas, best practice tips, professionally useful information
- actively participate in educational groups
- create a learning environment which is interactive, student-centred, authentic, collaborative, on-demand.

Catholic Education
Diocese of Parramatta

DON'T use social media networking tools to:

- model behaviour you would not encourage in students
- have an unprofessional profile picture
- play non-educational games
- engage in inappropriate online contact with students
- comment on students' non-school related posts
- share personal information that you wouldn't share in class - don't upload pictures of you drinking at a BBQ or in a bathing suit!
- discuss anything that is not education related
- denigrate or vilify others online.

DON'T allow students under the age of 13 to access social networking sites. Most sites (eg Google, Facebook, YouTube, etc.) will provide terms and conditions which provide details on age restrictions. You should check these terms and conditions before using with students. If you use social networking sites for educational instruction you may allow students between 13 and 18 years of age to access these under supervision. The type of supervision will depend upon the maturity of individual students.

Take care to ensure that any references to CEDP are factually correct and accurate and do not breach confidentiality requirements.

8. Privacy

Your privacy is important. So is everyone else's! CEDP will not usually disclose contents of emails and logs to external organisations unless required to do so by law. In the course of your work you may have access to or handle personal information about others, including students, colleagues, contractors, parents and suppliers.

The Privacy Act requires all in CEDP to take reasonable steps to protect personal information from misuse and unauthorised access. Our privacy procedures, disclosure of confidential information and record keeping process applies to handling of such information.

You are responsible for securing the computer assigned to you and for ensuring that it is not used by anyone who is not authorised to use it.

Take steps to secure password and log-on information, and ensure that your log-in code and password are not kept in your work area. You are encouraged to either lock your screen or log out when you leave your desk. This will avoid unauthorised access to your personal information, that of others and protect confidential information within your workplace.

You should familiarise yourself with the National Privacy Principles (NPPs) and ensure that your use of email and the CEDP network does not breach the Privacy Act or the NPPs. NPPs apply to staff emails and web browsing logs that contain private information. Exemptions apply to employee records. Improper use of email may pose a threat to system security, privacy of others and legal liability.

9. Distribution and copyright

When distributing information over the CEDP network, you must ensure that you and the school have the right to do so, and that you are not violating anyone's intellectual property rights. If you are unsure whether you have sufficient authorisation you should link to the source and attribute the source, rather than copying from it. Copyright law may apply to the information you intend to distribute. For this reason information downloaded from the internet (for example software, database files, documentation, cartoons, articles, graphic files and downloaded information) must not be distributed or broadcast through other digital communications (such as email or web pages) without specific permission to do so.

Most software, apps and online tools have associated licensing terms and conditions. You should read and comply with these before installing or using these tools on ICT.

10. Encryption and confidentiality

When digital content is created or stored on the network or the internet it may become public information. Encryption will reduce the risk of third parties being able to read this content and should be used in cases where you feel additional security is required.
Items of highly sensitive and secure nature should not be sent electronically unless encrypted. You should note that there is always a trail and a copy saved somewhere, not necessarily only on the CEDP network server.

This confidentiality requirement applies even when encryption is used.

You must ensure that your email address contains the CEDP's standard email disclaimer.

This message is set to appear automatically on each outgoing email. Please contact helpdesk if this feature is not working.
There is a risk of false attribution of digital communications. Software is widely available by which such communications may be edited to reflect an erroneous message or sender name.

The recipient may therefore be unaware that he or she is communicating with an impostor. Accordingly you should maintain a reasonable degree of caution regarding the identity of the sender of incoming communications. If you have concerns you should verify the identity of the sender by other means.

Please delete old messages and archive only those you need to keep. Retention of message fills up a large amount of storage space on the network server and can slow down performance. If there are items in the emails which you require at a later date, please ensure that these are saved in your network directory so that appropriate backups are made school wide.

11. Viruses, spyware and malicious software

The internet is a potential host for computer viruses, spyware and other software which may damage your device or place your personal identity and activities at risk. Downloading of infected information from the internet is potentially fatal to the computer network.
A document attached to an incoming email or clicking a link in an unknown message may result in malicious software being downloaded to your device.

Virus checking is done automatically through the virus protector software installed on the network server. If you are concerned about an email attachment, or believe that it has not been automatically scanned for viruses, you should contact helpdesk.

12. Absence

In cases where you are likely to be absent from work for a predictable period of time, you should set up an 'out of office reply' to ensure that those trying to contact you will be aware that you are not at work. Your out of office reply should contain the contact details of someone else who may be contacted in your absence.

13. General

ICT is continually changing. You will come across situations which are completely new to you, and may be new to many. The principles of common sense, respect for both the law and others, and promotion of the CEDP Strategic Intent will give a basis for the resolution of new situations.

14. What are the possible consequences for misusing ICT, the CEDP network and social media?

CEDP may take action to manage safety, conduct and performance in the workplace, including possible intervention, workplace direction, disciplinary action such as a warning, termination of employment or contract, notification to external agency, criminal charges. Misuse of ICT may have any of these consequences.

15. Relevant documents

- Communications Policy (being drafted)
- Stewardship Policy (being drafted)
- Staff Policy (being drafted)
- Responsible Use of ICT and Social Media - Procedures
- Responsible Use of ICT and Social Media Students - Guidelines
- Privacy Procedures
- Privacy Guidelines
- Parramatta Diocesan Privacy Policy
- Dignity and Respect in the Workplace Charter 2009
- Countering Discrimination Harassment and Bullying
- Procedural Fairness – Guidelines
- Addressing Unsatisfactory Performance
- Discipline Policy
- Workplace Health and Safety Manual