



USING DIGITAL COMMUNICATION
IN CAREER DEVELOPMENT PRACTICE

DISCLAIMER

The information contained in this document is for general information purposes only and is provided by the Career Industry Council of Australia. While every endeavour has been made to ensure the information is current at time of publication, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the information contained in the document. Any reliance you place on such information is therefore strictly at your own risk. You need to make your own enquiries to determine if the information is appropriate for your intended use.

In no event will we be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of information published in this document.

Please cite this document as: Career Industry Council of Australia (2021). Using Digital Communication in Career Development Practice. Career Industry Council of Australia, Melbourne. Available from: www.cica.org.au

TABLE OF CONTENTS

INTRODUCTION	4
WHAT IS DIGITAL COMMUNICATION?.....	5
ADOPTING DIGITAL COMMUNICATION	6
USING DIGITAL COMMUNICATION	7
APPENDIX 1	9
APPENDIX 2	11
APPENDIX 3	12

INTRODUCTION

With advances in technology, digital communication is an accepted norm in career development services, and there is an expectation that it is competently and ethically integrated into practice by career development practitioners. In the context of increased use of digital communication in career development services, this document is not intended as a set of comprehensive guidelines about the use of digital communication. Instead, it is intended to stimulate reflection and discussion by career development practitioners on the adoption and integration of digital communication into practice.

To assist career development practitioners, primarily those new to using digital communication in their client services, this document draws attention to some points for career development practitioners to consider about making the best use of communication technology while protecting themselves and their clients. This document about using digital communication in practice complements the Professional Standards for Australian Career Development Practitioners.

The Professional Standards apply to all forms of practice, including the use of digital communication.

Each CICA Member Association has a Code of Ethics that accords with the CICA Professional Standards and career development practitioners.

No matter what type of service career development practitioners offer, are expected to abide by the Code of Ethics of their professional association. In particular, practitioners who work with children or vulnerable people need to consider additional ethical and legal obligations regarding informed consent, privacy, and probity.

After briefly considering what digital communication is, this document is presented in two sections. The first section, Adopting Digital Communication, invites career development practitioners to reflect on the introduction of digital communication into their practice. The second section, Using Digital Communication, invites career development practitioners to reflect on their application of digital communication in their practice.

Accompanying appendices provide more specific points for consideration.

WHAT IS DIGITAL COMMUNICATION?

Digital communication refers to a range of technologies that enable practitioners to communicate with clients. Technologies include, but are not limited to:

- Phone (smartphone)
- Email
- Text messaging
- Real-time Chat
- Asynchronous text
- Webcam/videoconferencing
- Virtual reality and gaming
- Online Evaluation and Assessment
- Discussion boards and forums

Some technologies enable digital communication in real-time, i.e., the career development practitioner and their client are communicating through their computer or phone at the same time (e.g., Microsoft Teams, Google Hangouts, Zoom, Messenger or WhatsApp video calls). This method is referred to as synchronous communication.

Other technologies such as text-based technologies (e.g., email, messaging platforms such as Messenger or WhatsApp chat) may result in time delays because the career development practitioner and the client do not have to be using their phone or computer at the same time. This method is referred to as asynchronous communication.

ADOPTING DIGITAL COMMUNICATION

In considering the adoption of digital communication into practice and which technologies to adopt, career development practitioners need to consider their current level of comfort and competency as well as their willingness to learn and adapt. Some practitioners are enthusiasts who embrace new forms of technology. Others are more cautious, or maybe even reluctant, to use any form of technology at all. Choosing to offer services through digital communication depends on a practitioner's preferences and levels of familiarity and comfort with various technologies, their access to and familiarity with the technologies on offer, the technologies available through their workplace, and client needs. Each form of digital communication brings its own set of considerations (See Appendix 1).

Some practitioners work independently and are responsible for managing their adoption and use of technology. Others work in organisations which have policies, systems, and support services to help practitioners with using digital communication. For example, career development practitioners working in schools or universities should always check with school principals, line managers, technology support staff, and any applicable governing or regulating bodies about the policies and procedures which apply to the use of digital communication technology in the workplace, associated risk management, privacy and informed consent. Organisations may have policies about which technologies can be used and by whom.

Before adopting digital communication in practice, undertaking a needs analysis about how using digital communication could enhance practice is advisable. Practitioners need to know their level of competency in the use of digital communication and should not use technologies with which they are unfamiliar. Developing skills in the use of digital communication allows practitioners to build confidence and assists them to understand better the ethical, privacy and security issues associated with its use. Career development practitioners should carefully consider the incorporation of technology into practice and the privacy of any technology platform before they consider its use as part of their practice. The following questions may guide such consideration.

- What forms of technology are you familiar with and comfortable to use with clients?
- Which technology choices could you offer depending on client needs, preferences and level of familiarity and comfort?
- If your organisation mandates the use of specific technologies, how can you increase your skill and confidence in utilising the technologies required in your practice?
- If you work with children, how will your choice of technology impact privacy and consent considerations for the child and their parents or caregivers?
- How does the technology meet the needs of your practice?
- How will the use of this technology impact the work you undertake with a client?
- What strategies will you implement to mitigate any negative impact?
- What is the evidence base for the technology?
- Have you tested the technology to determine what it is like to use, how it functions and whether it meets your needs and requirements?

USING DIGITAL COMMUNICATION

Having an understanding of and competency in how digital communication works is vital for career development practitioners. Consideration needs to be given to security, privacy, informed consent, risk management, and insurance.

SECURITY

Security of digital communication may be enhanced in several ways including encryption, account management, backup systems, password protection, firewalls, virus protection, hardware, software, and understanding third-party services (See Appendix 2 for further information).

PRIVACY

Privacy is an essential consideration in the use of any form of technology. Privacy laws have been developed at national, state and territory levels and by some organisations to ensure legal compliance. Carefully read the privacy policies of the technology platforms you are considering. Consider conducting a Privacy Impact Assessment (PIA) for each technology use and client group you work with (see Appendix 3 for an example of a Privacy Impact Assessment).

INFORMED CONSENT

When using digital communication, there are additional considerations regarding informed consent. It is essential to include the following:

- Be clear about how you work online, i.e., expectations of client and client expectations of career development practitioner
- Clarify with clients when you are and are not available. Inform clients on how you will communicate between sessions if indeed there will be any communication
- Technological glitches happen. Make sure that you have back up communication and emergency procedures, especially if you plan on using real-time communication technologies
- Just as in face-to-face counselling miscommunication happens. Let clients know how to handle any miscommunication or misunderstanding they may experience
- Ensure clients understand the importance of the privacy of communications with you (e.g., not copying others or forwarding to others)
- Consider whether you want to restrict copying and pasting of your work (e.g., whether or not you would be okay with a client copying and pasting your comments as their new Facebook status)
- Clarify with clients that they agree not to misrepresent their identity.

RISK MANAGEMENT

Risk management concerns identifying, assessing, and controlling for any risks that may eventuate from your practice. Career development practitioners need a basic understanding of risk management, including an understanding of where their data is stored. Career development practitioners must ensure the privacy and confidentiality of their clients and any data they may collect from them. A responsibility of career development practitioners is to demonstrate that they have recognised the risks and have taken reasonable precautions to prevent them from causing harm to their clients, property, or reputation.

INSURANCE

Career development practitioners, especially those working in private practice, should hold professional indemnity insurance. It is advisable to check with your insurance company to see if your policy covers services provided through the forms of digital communication you use, where you are delivering those activities from, and where your clients are located when you are providing those services. In some cases, your existing policy will cover these activities, while other providers will require you to purchase an additional rider to cover these activities. Also, check that your insurance covers you for cybersecurity and privacy liability. In some cases, you may want to inquire about coverage that extends beyond professional liability.

The use of digital communication in career development services is here to stay, and the onus is on career development practitioners to competently and ethically integrate it into their practice. This document is designed to stimulate reflection and discussion by career development practitioners on the adoption and integration of digital communication into practice.

APPENDIX 1

Considerations for Using Digital Communication Technologies

Each form of digital communication raises its own set of considerations.

TELEPHONE

- Consider the privacy of where you make calls from and minimise or eliminate interruptions and background noise
- Be aware of the tone and pitch of your voice
- Use more frequent vocalisations to indicate you are listening.
- Avoid using your own personal mobile phone where possible. Try to have a separate number/phone for making calls to clients or switch your phone to private so that your number is not shown or know how to block your number when you make a call on your personal mobile to a client.

EMAIL

- Have a secure and separate email address for clients
- Encrypt all email used to communicate with clients. Options include:
 - Encrypt or password-protect a document that you are sending to a client;
 - Encrypt or password-protect the email itself;
 - Use a secure, encrypted email system to communicate with or provide information to clients.

Clients may say they want unencrypted email communication though they may not fully understand the privacy implications.

TEXT MESSAGING

- Use a secure text messaging option
- Be clear about what you will use text messaging for – appointment changes? Reminders? Check-ins?
- Clarify the times that you will be available/contactable in regular business hours
- Clarify your client's view of texting
- Speed makes a difference in text messaging, and it can easily be misconstrued if something takes longer than the client anticipates
- Understand how emoticons and abbreviations are used
- Know the current slang for text messaging
- Be professional - understand the slang, but to avoid misunderstanding, avoid using slang, even if clients use it when texting you
- Ensure arriving text messages don't appear on your screen, potentially compromising confidentiality.

REAL-TIME CHAT

- Requires a different type of focus and patience
- Close all other applications
- Eliminate interruptions
- Most of the considerations in the above section on texting apply here.

ASYNCHRONOUS TEXT-BASED COUNSELLING

- Use an encrypted system
- Use presence techniques to assist with a lack of visual cues and to enhance the sense of experiencing the session in the moment
- Set your boundaries for working online, e.g., define availability, after-hours work
- Pay attention to how much time you spend on a session
- Take care in translating counselling words/language into text.

WEBCAM/VIDEO

- Use a secure encrypted platform
- Consider your bandwidth, lighting, background, clothing
- Note the quality of your headset, reliability of sound/audio
- Check the capability/compatibility of your client's device
- Use a unique meeting sign-in with a password for each client rather than a recurring meeting "room" where other clients may enter during a prior session if they arrive early
- Agree with the client on contingencies if the connection drops out, the screen freezes and other technical difficulties. Options could include moving to camera off, reverting to phone or tethering to mobile rather than WIFI
- Consider practicalities such as who else can hear the conversation, who else might be in, or enter, the room
- Consider the ethics of your practice, e.g., will you be recording sessions and does the client receive a copy of the recording? If so, can they post portions to the Internet?
- Seek prior permission to record a webinar or session through a client consent form
- What considerations do you have in place for accessibility for people with disabilities, with digital inequities, a slow connection in regional and remote areas.

APPENDIX 2

SECURITY

- Account management relates to maintaining multiple accounts in the same platform and switching between them appropriately, i.e., a personal and a professional email or Facebook account
- Backup systems assist in the secure storage of records and data on your own system or via a secure, encrypted system. Examples include external hard drives and cloud storage.
- Encryption is a way of encoding a message or file so that it can be only be read by the people it is intended for.
- Firewalls are security systems installed on networks according to a set of rules that monitor and control incoming and outgoing network traffic.
- Password protection is a form of security that protects information by only allowing access to users with a secure password. Strong passwords generally include a combination of uppercase and lowercase letters, numbers and special symbols, such as punctuation. Some other forms of password protection include password manager programs and using 2-Factor Authentication.
- Third-party services are sometimes used by digital service providers to store data (e.g., in a cloud, in Australia or overseas). These third-party services may determine how data are used and who has access.
- Virus protection protects your computer and your files from attack from unknown sources.

Examples of Privacy Impact Assessment Questions

PRIVACY IMPACT ASSESSMENT QUESTIONS TO CONSIDER

- What personal information (e.g., client names, contact information) will be collected, and how will it be used?
- Who will see or have access to the personal information that is collected?
- How will you make your clients aware of how their data may be collected and used, and gain their consent?
- What measures are in place should a client request their data be removed from the system? or should a client request access to their data?
- Will personal information be shared?
- Do the technology platform developers have access to any information that you are collecting?
- Where are the data stored? Are the data stored on your organisation's server or an external server, or are the data stored in the Cloud, hosted in Australia or internationally?
- What are the privacy laws in my State or Territory?
- How are the data transmitted? Is it encrypted?
- Does the technology require password protection? Is 2-Factor Authentication available?
- Is your hardware located in a secure premise?
- Can you turn off any features that collect data, or can users request access to or deletion of their data?
- If records exist with third parties (e.g., telecommunication provider, cloud provider), are those records deleted when you delete them on your device (e.g., laptop, computer, tablet, phone)?
- Do I have a plan for how to handle privacy and security breaches if they occur? Whom will you need to contact and when? What are the risks to clients? What are the potential harms if a breach occurs? How can these risks be mitigated?