Privacy and You

For staff of DCJ contracted service providers

Course overview

- This course will outline what privacy is and why it is important to you. It is designed for employees of DCJ contracted community service organisations.
- In this course, you will learn:
  - How our privacy obligations applies to you
  - What it means to comply with privacy legislation
  - What the consequences are for not complying with privacy legislation
  - How to manage personal information on a day to day basis
  - What type of information is sensitive
  - What to do if it goes wrong – who to tell and what steps to take

What is privacy?

- Privacy is the **responsible and lawful handling** of all personal and health information held by you and your organisation. It refers to all dealings of information, from the point of collection through to use, storage and disposal.
- While **confidentiality** and **security** are important aspects of privacy, they are only part of it. Privacy includes being **transparent, accountable** and **ethical** in the way you handle information.
- Privacy requires you to think about why and how you collect and handle information in your day to day work. This includes obtaining consent, providing notice and advising a person why you are collecting their information.

What is privacy? (cont.)

There are two types of information covered by privacy legislation:

- **Personal** – information or an opinion about an individual whose identity is apparent or can be reasonably ascertained (e.g. names, signatures, addresses, opinions, medical and health information, photographs, CCTV)
- **Health** – information or an opinion about a person's physical or mental health or disability, their express wishes about the future provision of health services, or details of past or future health services (e.g. physical health, mental health, disability, organ donor status, medical appointments)

Why is privacy important?

- Privacy builds **trust** between you and the communities you work with. It assures a person that you and your organisation will handle information about their life and identity carefully.
- Privacy ensures the **security** and **safeguarding** of personal information and helps prevent unauthorised access, misuse or disclosure of information.
- You and your organisation have **contractual** and **legal obligations** to comply with the below legislation. NSW government agencies, including DCJ and organisations providing services on DCJ's behalf, must comply with the following legislation:
  - NSW Privacy and Personal Information Protection Act 1998 (PPIP Act)
  - NSW Health Records and Information Privacy Act 2002 (HRIP Act)
  - NSW Government Information (Public Access) Act 2009 (GIPA Act)

Privacy principles

The Information Protection Principles outline how to handle personal information in your day to day work.

1. **Collection** – only collect what is necessary and relevant to the delivery of your service. Information should be sourced directly from the individual, where possible. You must provide a privacy notice that outlines how the information may be used.
2. **Use** – ensure the personal information is accurate and up to date. Personal information must not be used for unrelated purposes such as advertising, marketing or research. Consider the following questions:
    - Why was the information collected?
    - How long ago was it collected?
    - Is the information still accurate?
    - Is my proposed use related to the purpose of collection?

Privacy principles (cont.)

3. Disclosure – only disclose information to another person or agency when it is required by law, it relates directly to the original purpose of collection, the individual has given you consent, or there is a serious/impending threat to a person's life or health. Ensure necessary redactions are done accurately.

4. Storage and security – you must store personal information securely to prevent loss, misuse and unauthorised disclosure. Information must not be stored on personal devices or other systems unless approved. You should adopt appropriate security measures, such as restricted access to files. Information must be disposed when it is no longer required. The fact that information is not stored securely is a breach of privacy legislation, regardless of whether the information is actually lost or disclosed.

Privacy principles (cont.)

5. Access and amendment – individuals have the right to request access to their personal information. Access must be provided within a reasonable timeframe. An individual can also ask for an amendment to their personal information. Contracted service providers should contact their contract manager regarding access and amendment requests when concerned that the information is contentious or sensitive.

What is a privacy breach?

- A **privacy/data breach** is when personal information is lost, misused, or unlawfully disclosed, regardless of whether the breach is intentional or accidental.
- This could be as a result of a file or computer being lost or stolen, information being sent to the wrong recipient, or a malicious or hacking event. This is known as a **privacy/data breach** under the PPIP Act.
- Some examples may include:
  - deliberate interference with, or unauthorised access of electronic or physical records
  - loss of electronic and/or physical records as a result of a fire or flood
  - theft or loss of mobile storage devices, such as a USB or laptop
  - an email involving client information sent to the wrong person
  - unauthorised staff accidentally or deliberately accessing restricted documents
  - improperly providing access to, or sharing, sensitive information with a third party

What is a privacy breach? (cont.)

- It is important that you understand the procedures relating to privacy/data breaches. These procedures outline who to notify and what steps will be taken to contain, assess, investigate and respond to the breach.
- When any privacy breach is first identified, you should **act quickly** to minimise actual or potential harm to affected individuals.

What about privacy complaints?

- Individuals have the right to make **complaints** or **allegations** that you or your organisation have breached their privacy.
- You should refer to your organisation's procedures for assessing and resolving privacy complaints. Where a complaint is serious or complex, or the applicant seeks review of the alleged breach, contracted service providers should contact their contract manager.
- Resolving privacy complaints may include apologising, explaining why the action occurred and/or rectifying the issue with the support of your manager.

When to notify the Department

- If there is a privacy/data breach where any DCJ information may have been compromised or lost, your organisation must notify DCJ Cyber Security and your contract manager immediately.
- Details of the breach should be submitted via the online notification form.
- Your organisation will work with DCJ to:
  - investigate the nature and extent of the breach
  - assess the risks and consequences associated with the breach
  - notify relevant regulators (NSW Information and Privacy Commission, the Office of the Australian Information Commissioner, Cyber Security NSW)
  - review the circumstances and participate in action to mitigate the risk of any future breach

MNDB Scheme Overview

- From 28 November 2023, DCJ is required to notify the Privacy Commissioner and affected individuals of all **eligible data breaches** involving personal or health information.
- An **eligible breach** occurs where there is unauthorised access, disclosure or loss of personal information, that is likely to result in serious harm. Examples include:
  - Loss or theft of a device containing DCJ information
  - Mistakenly providing personal information to an unauthorised person
  - Sending an email containing personal information to an unrelated third party
- Serious harm includes physical, financial, material, emotional or psychological harm

Case study 1

- Scenario: Hanadi arranges a Zoom meeting with her team. The meeting will involve discussing sensitive personal information of DCJ clients. She joins the meeting remotely at a local coffee shop.
- Challenge: Hanadi and her organisation have ongoing obligations to maintain the security of the personal information of DCJ clients. She must consider the potential risks of discussing personal information in a public setting, which may result in an inadvertent disclosure.
- Solution: Hanadi should follow her organisational procedures and join the meeting from an approved location. It must be a private environment, such as her work office, home or other private and secure space. If Hanadi is concerned her meeting may still be overheard, she should avoid mentioning any information that may identify the client, such as names or addresses.

Case study 2

- Scenario: Mario sends an email containing personal information of a DCJ client to his contract manager. The email included the name and address of the client and the type of service they received. Shortly after, he realises he has sent it to the wrong person.
- Challenge: By sending personal client information to the wrong person, Mario has caused an accidental data breach. Mario needs to address the incident quickly and take appropriate actions to minimise any actual or potential harm.
- Solution: Mario must immediately notify his supervisor and contract manager. He should also follow any organisational procedures to responding to a breach, and consider any immediate steps he could take to retrieve the information or minimise harm. For example, if the email was sent to an unrelated third party or a different organisation, Mario could contact the recipient and ask them to delete the email without accessing or distributing its contents.

Case study 3

- Scenario: Jordan is out of the office for the day, conducting a number of home visits with DCJ clients. Jordan brings the client's file to the home visit, and carries with the file from the previous client's visit. Both files contain personal information. After finishing up the visit, they leave the previous client's file behind inadvertently.
- Challenge: By inadvertently leaving the previous client's file, Jordan has caused an accidental data breach and potentially exposed their previous client to serious harm.
- Solution: Jordan should immediately return to the home visit and request the physical file be handed back. Jordan must immediately notify their supervisor and contract manager. They should also follow any organisational procedures to responding to a breach. In future, Jordan and their organisation should consider different procedures when conducting home visits, such as leaving the files of previous clients locked in the car, or only taking digital copies of files to home visits on protected organisational devices.

For more information

- Learn how to keep information safe and respond to an incident in the Information Security Training Resource
- Review the Key Privacy Obligations Factsheet
- Understand your responsibilities in our policy for Maintaining secure information and notifying us of information security incidents