

Privacy for Charities and Not-for-Profits: Tips and Tricks

Louisa Joblin

Special Counsel (Privacy and Not-For-Profit), Duncan Cotterill

Jo Cribb

Consultant, JoCribb.co.nz

Eve Kennedy

Manager, Capability and Guidance (OPC)

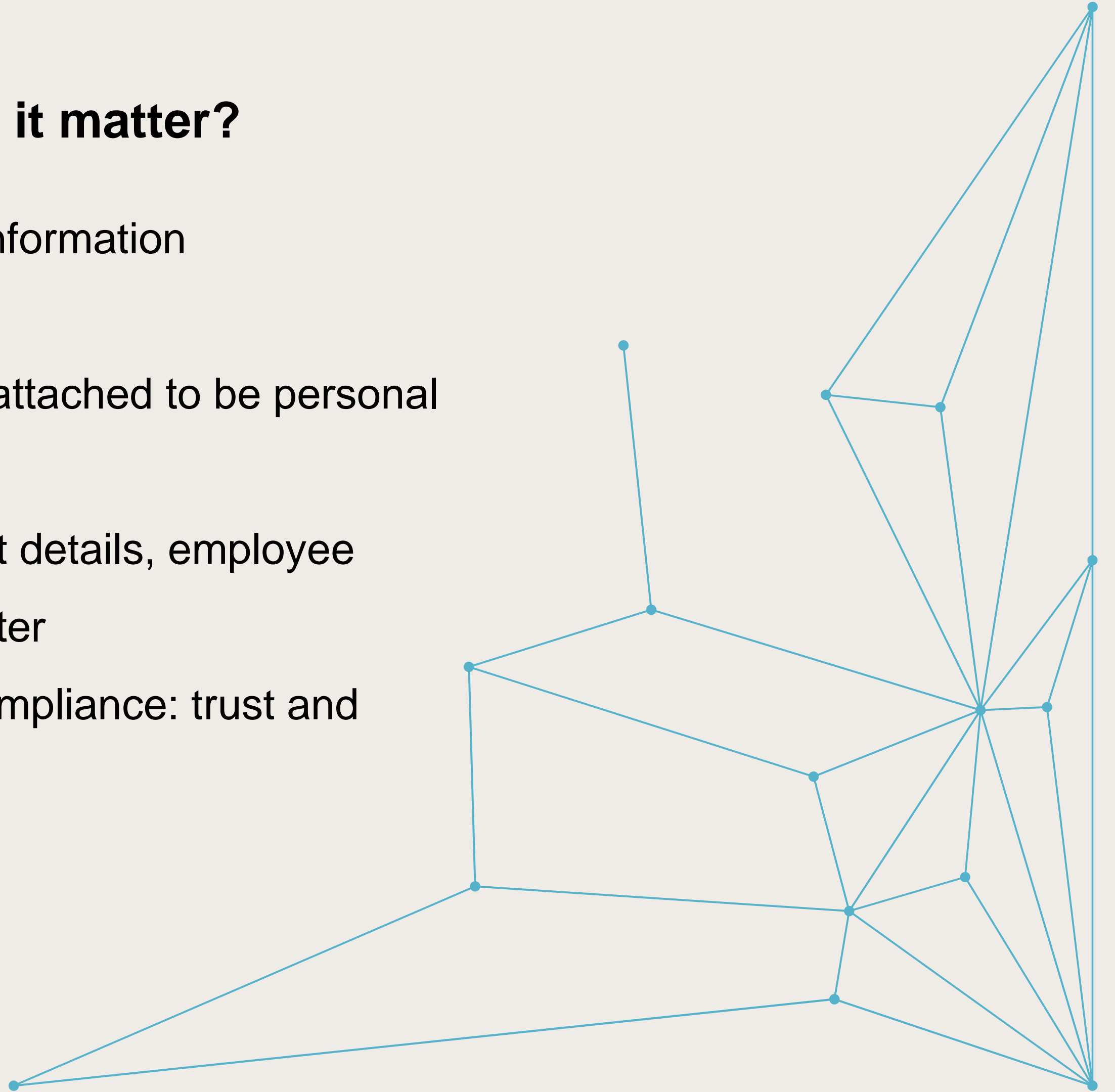


This webinar will cover:

- What is privacy and why does it matter?
- Overview of the information privacy principles under the Privacy Act 2020
- Notifiable privacy breaches
- Having a privacy officer
- Where to start? Tips and tricks
 - 8 questions to ask at your next board meeting

What is privacy and why does it matter?

- Privacy Act is all about personal information
 - Broad definition
 - Doesn't need to have a name attached to be personal information
 - Includes photos, notes, contact details, employee information, format doesn't matter
- Privacy is more than just legal compliance: trust and confidence



Who we regulate

You.

The Privacy Act 2020 applies to...

- any public or private sector agency that collects or holds personal information
- the actions of agencies, both within New Zealand and outside of it

‘Agency’ is defined in the Act as any business, group, or organisation that collects personal information. (s 8)

It can include an individual where an individual undertakes those activities (eg sole trader), but not when it involves their domestic or personal affairs.

There are some exceptions

News media in relation to news gathering activities; judicial functions of the Court/Tribunals, Governor-General, Parliament, Ombudsman Offices



Privacy Act 2020: Privacy Principles

Collecting Personal Information

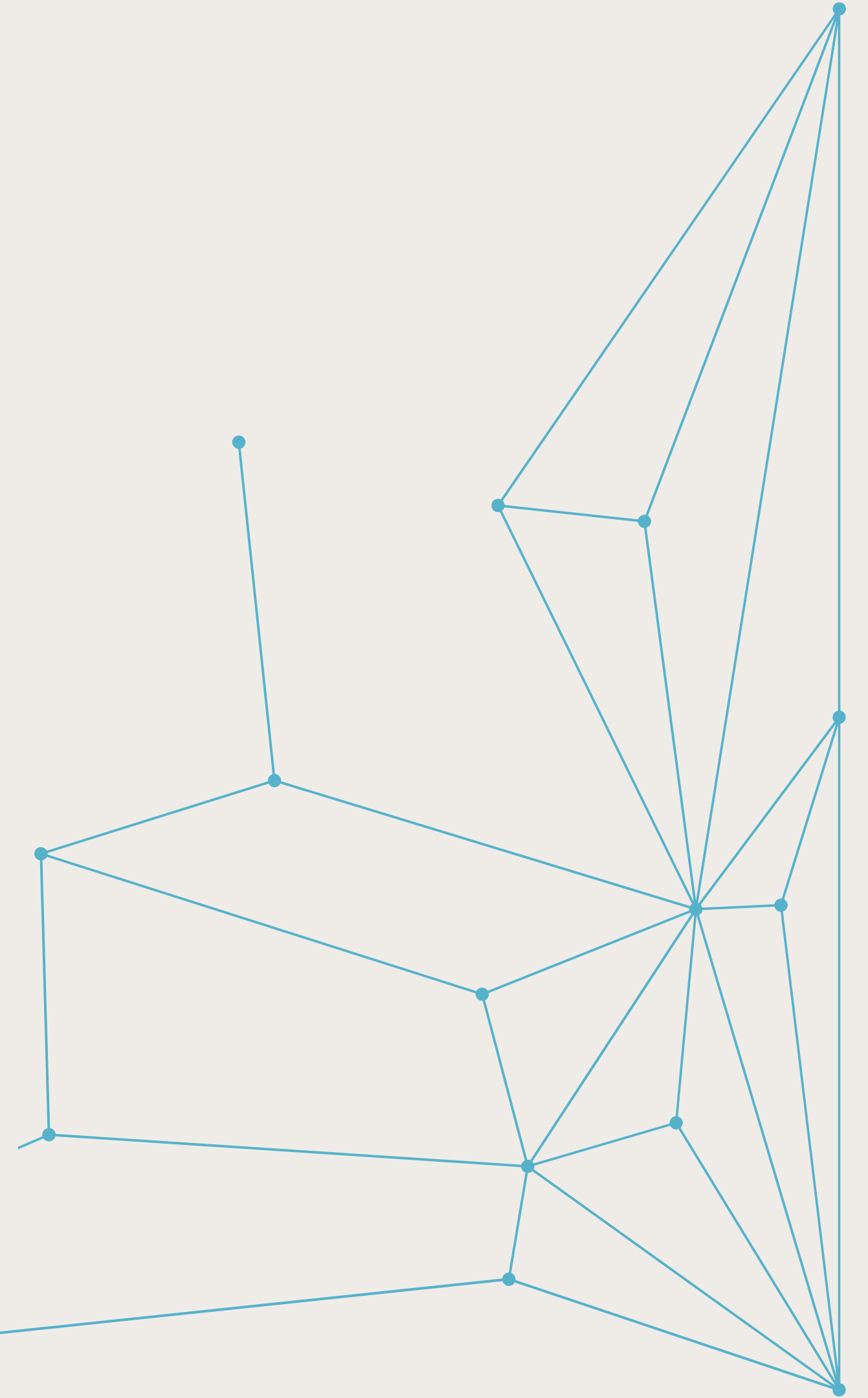
1. Only collect personal information you **need**
2. Get it **directly** from the person when possible
3. Be **Open** about what you are going to do with it
4. Be **Fair** about how you get it

Holding Personal Information

5. Keep it **Secure**
6. Let people **see** their own information
7. **Correct** it if the person thinks it's wrong

Using and Disclosing Personal Information

8. Make sure it is **accurate** before using it
9. **Dispose** of it when you no longer need it
10. Only **use** it for the reason it was collected
11. Only **share** it if you have good reason
12. Only send it **overseas** if it will be protected
13. Only use **unique identifiers** when permitted



Privacy Breaches

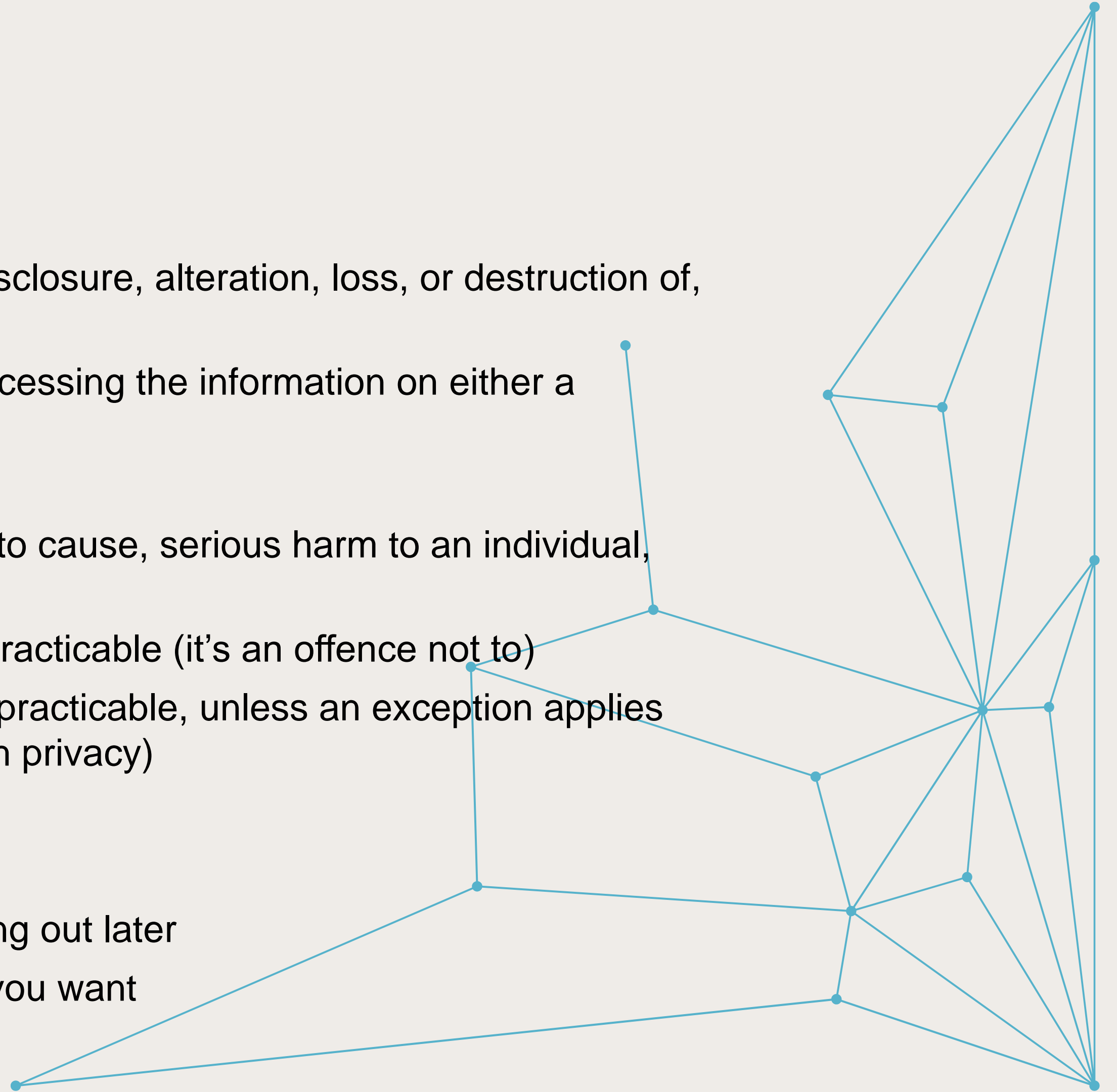
A **privacy breach** is:

- Unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, the personal information; or
- An action that prevents the agency from accessing the information on either a temporary or permanent basis

A privacy breach that has caused, or is likely to cause, serious harm to an individual, agencies is a **notifiable privacy breach**

- Must notify the Commissioner as soon as practicable (it's an offence not to)
- Must notify affected individuals as soon as practicable, unless an exception applies (failure to notify may be an interference with privacy)
- Information may be provided incrementally

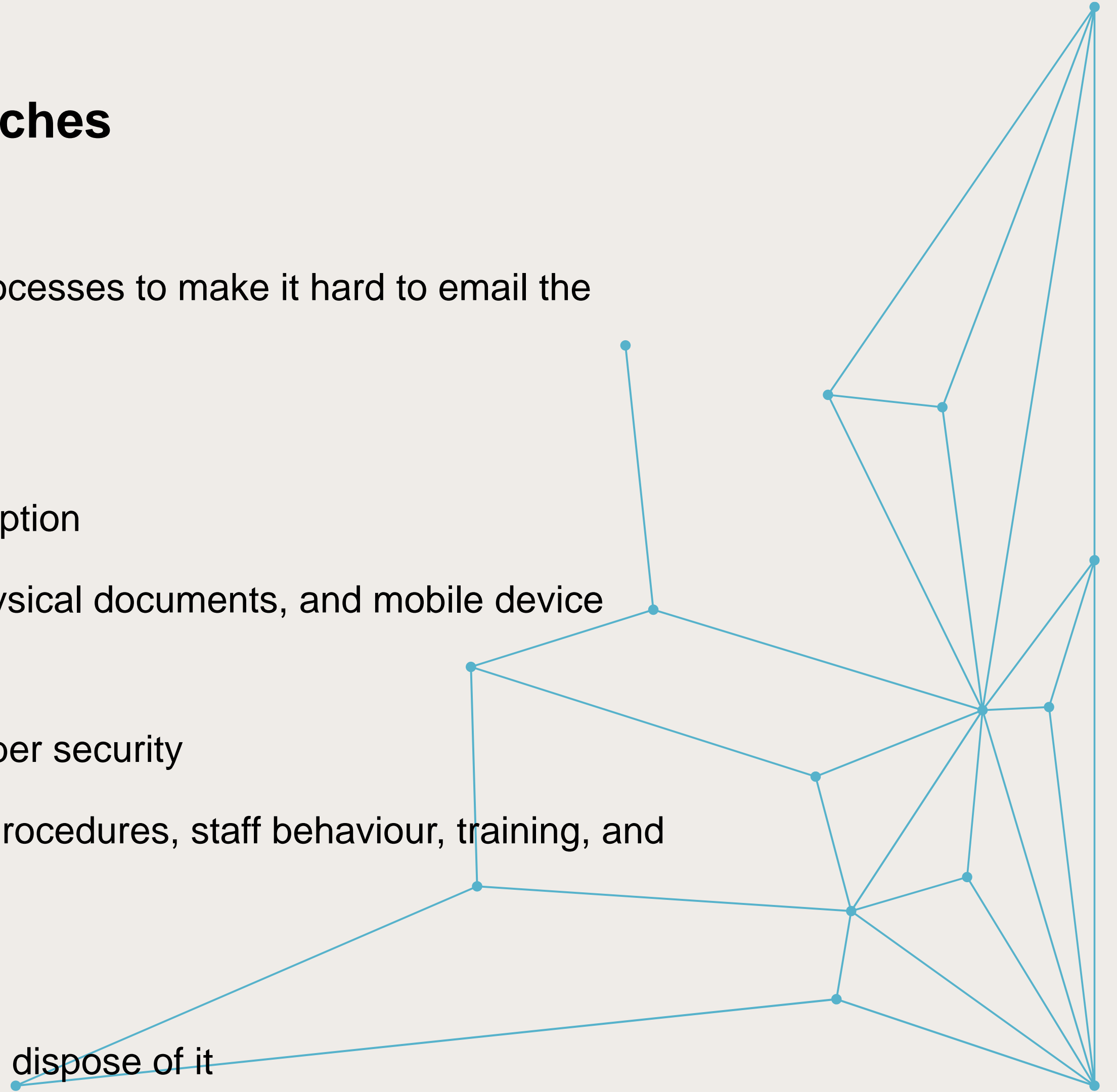
Draft guidance on breach management coming out later this month; email poupou@privacy.org.nz if you want to be on the mailing list to get it.



Preventing Privacy Breaches

How to prevent it happening again:

- Changes to email systems and business processes to make it hard to email the wrong thing to the wrong person
- Pause, check, check again
- Protect information with passwords or encryption
- Physical – for example, building access, physical documents, and mobile device protection
- Technical – for example, IT systems and cyber security
- Organisational – for example, policies and procedures, staff behaviour, training, and awareness
- Staff training
- Know the information you hold, and when to dispose of it

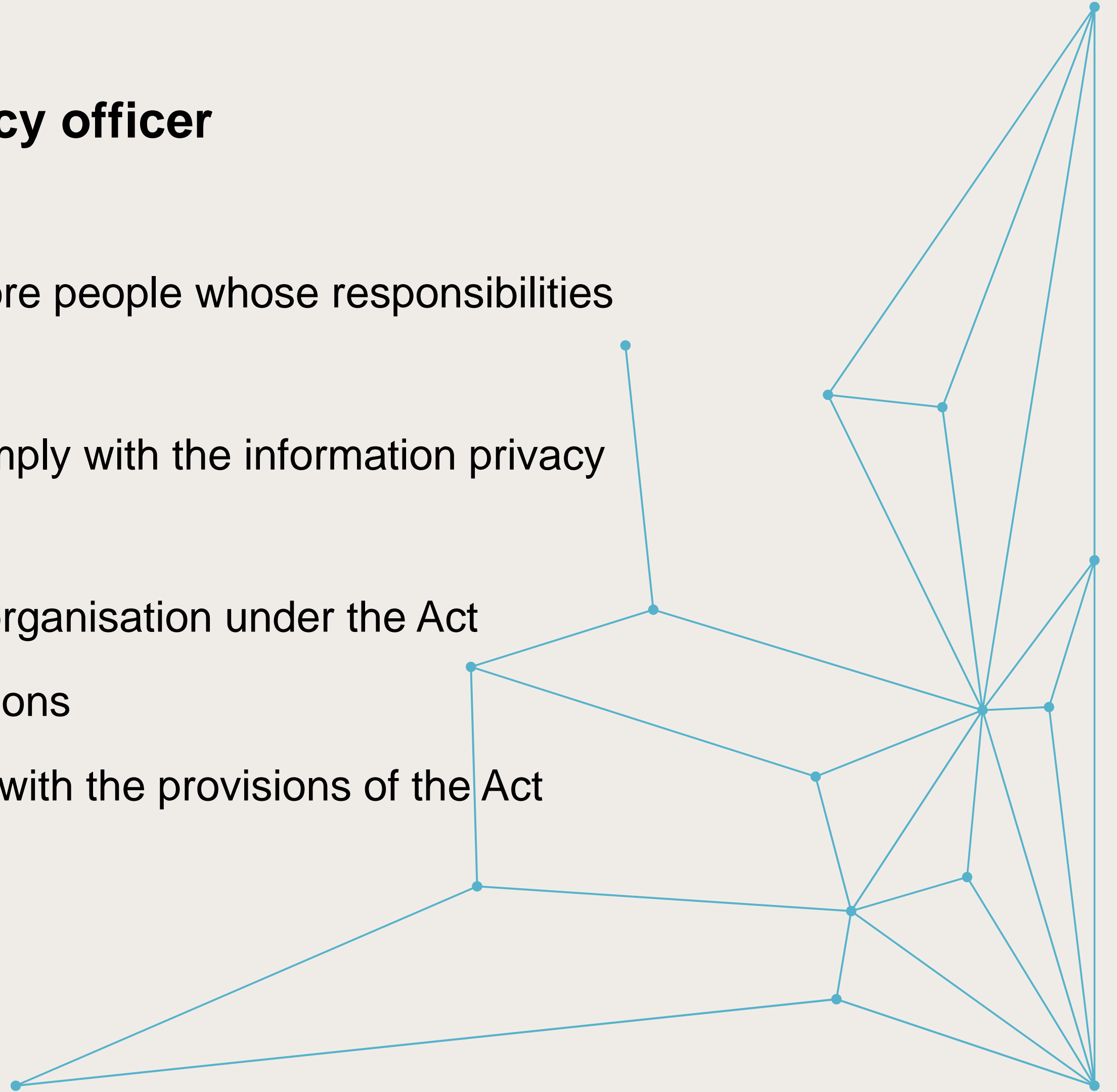


Requirement to have a privacy officer

Section 201 of the Privacy Act

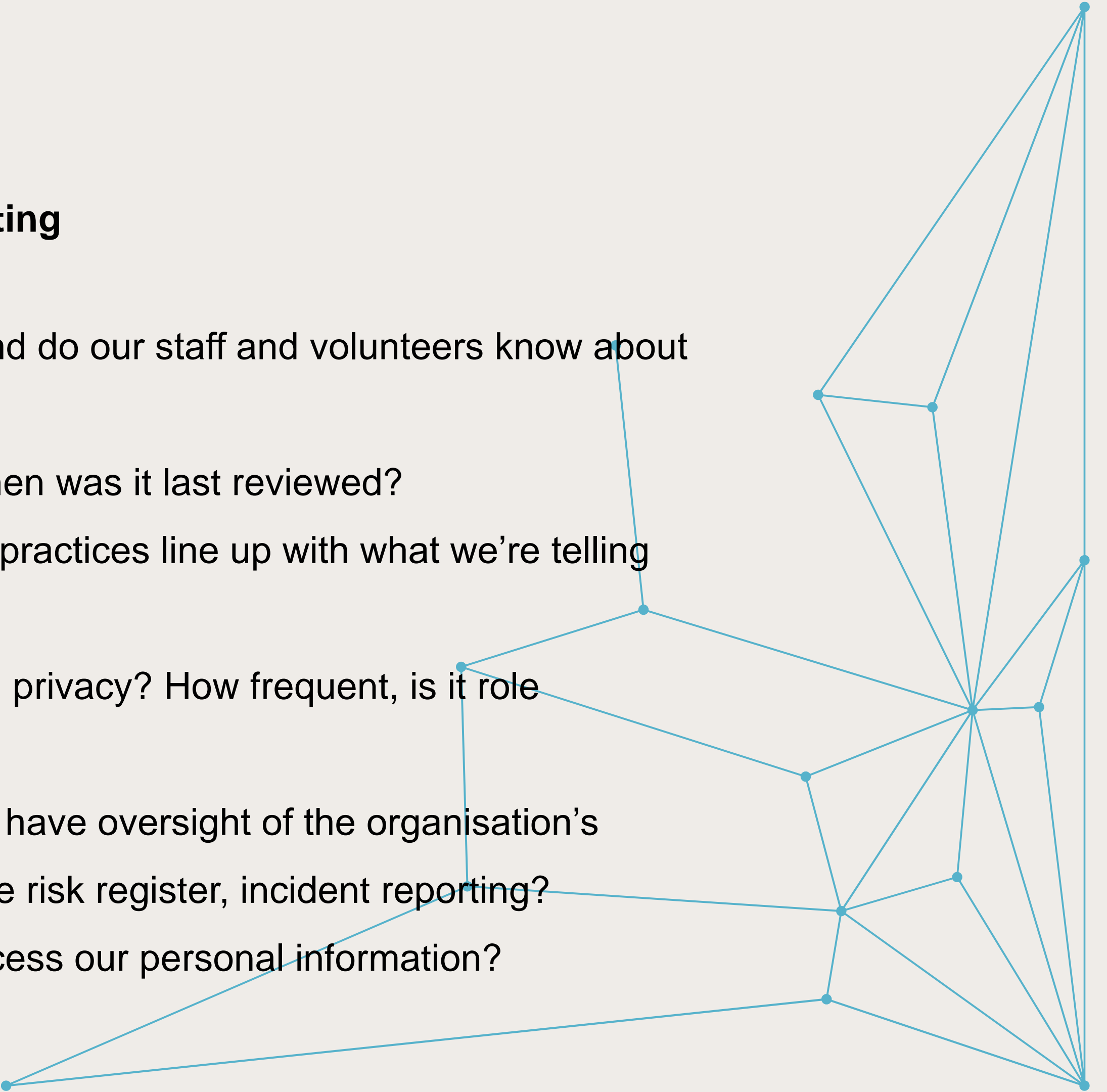
Each organisation must appoint 1 or more people whose responsibilities include:

- Encouraging the organisation to comply with the information privacy principles
- Dealing with requests made to the organisation under the Act
- Working with OPC during investigations
- Ensuring the organisation complies with the provisions of the Act



Where to start:

8 questions to ask at your next Board meeting

- What personal information do we hold?
 - Who is the organisation's privacy officer, and do our staff and volunteers know about them?
 - What do we have in our privacy policy? When was it last reviewed?
 - Do our organisation's information handling practices line up with what we're telling people?
 - What training do our staff/volunteers get on privacy? How frequent, is it role specific?
 - How will we as a Board/Governance group have oversight of the organisation's privacy risks? E.g. is privacy covered on the risk register, incident reporting?
 - What service providers do we use that process our personal information?
 - Do we have a breach management plan?
- 



Privacy Commissioner
Te Mana Mātāpono Matatapu