

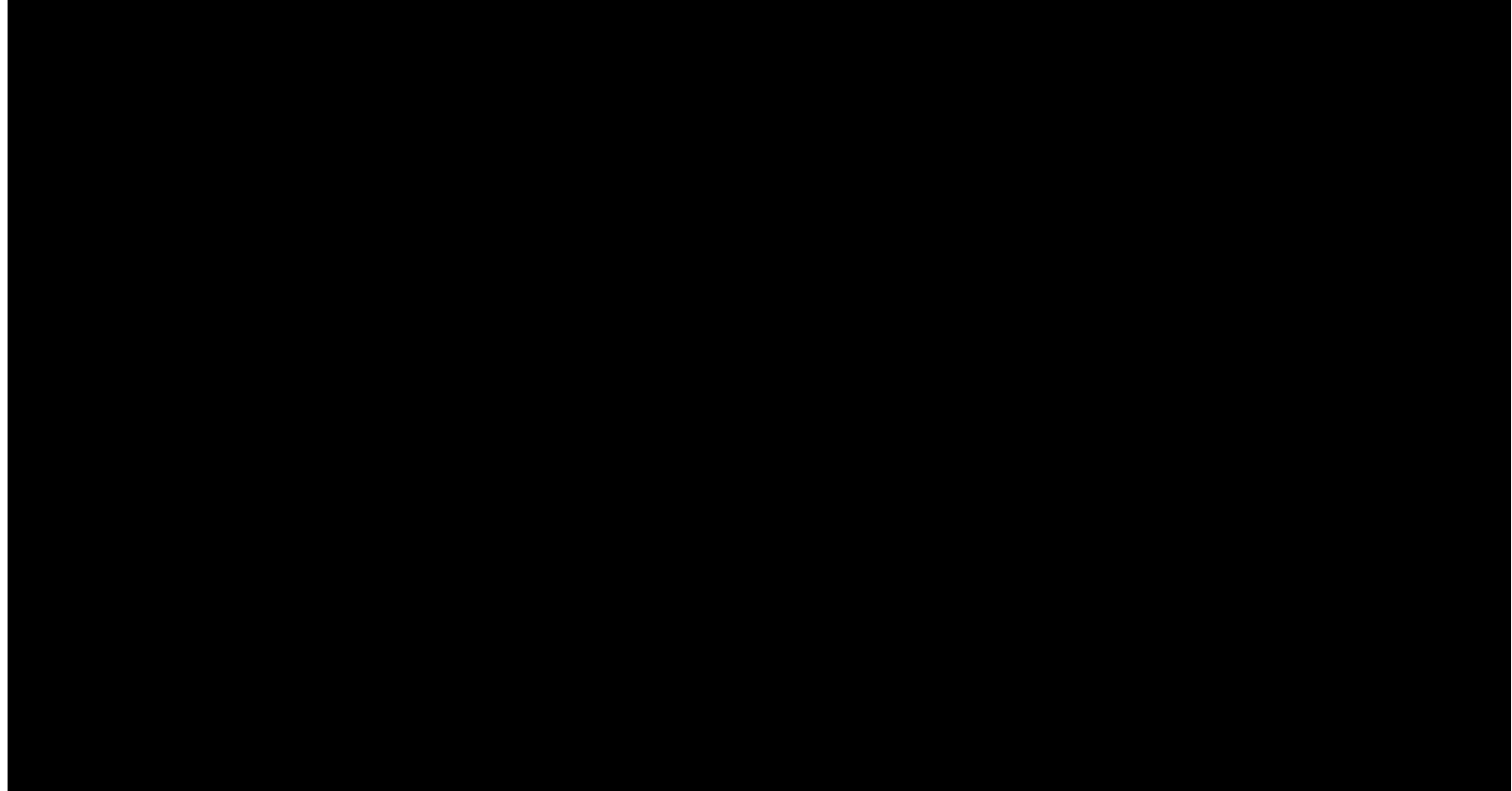
Privacy and Freedom of Information (New Starter)



The purpose of this module is to provide you with an overview of the Office of the Fair Work Ombudsman (OFWO) **privacy and freedom of information protocols**.

- ☰ Introduction
- ☰ Overview
- ☰ The Australian Privacy Principles
- ☰ Identifying personal information
- ☰ Applying the Privacy Principles in your role
- ☰ Privacy breaches
- ☰ Privacy knowledge check

s.22 Irrelevant Information



Documents released by the
Under the Freedom of Information Act

Lesson 1 of 10

Introduction



The journey towards reconciliation, Jordan Lovegrove

The Fair Work Ombudsman acknowledges the Traditional Custodians of Country throughout Australia and their continuing connection to land, waters and community.

We pay our respect to them and their cultures, and Elders, past, present and future.

The purpose of this module is to provide you with an overview of the Office of the Fair Work Ombudsman (OFWO) **privacy and freedom of information protocols**.



“Learning outcomes

After completing this module, you will be able to:

- identify information defined as personal
- explain how privacy affects your work
- understand where you fit in the FOI process
- explain your role in our response to FOI requests.



“Duration

You should allow **25 minutes** to complete this module.”

CONTINUE

Overview



“CONSIDER

Would it make you feel uncomfortable if people you do not know could find your contact details or knew where you live?

Imagine if your health records were something people could look up at their leisure?

I bet it fills you with dread! And so it should.”

Private sign

Luckily, we all have the legal right to have our personal information protected.

The Privacy Act 1988 (Privacy Act) protects your privacy by setting rules for how government and some businesses collect and handle your personal information.



“CONSIDER

Now, let's think about the role of the Office of the Fair Work Ombudsman (OFWO). We collect and investigate a broad range of personal information to provide our service to the Australian public.

We must follow the requirements set out in the Privacy Act to safeguard personal information.”

We also need to look after the personal information we keep for OFWO staff.

We collect your information for activities such as:

- your police check from when you started out here in the OFWO
- documents you provide to access your leave entitlements.

This learning provides you with the information you need to know to help keep the personal information of the Australian public (including yours and your coworkers) protected.

CONTINUE

The Australian Privacy Principles

The Privacy Act provides us with the Australian Privacy principles (APP), described as 'the cornerstone of the privacy protection framework in the Privacy Act'. The APPs provide us with clear privacy guidelines in plain English terms.



"MORE INFORMATION

You should review the APPs on the Office of the Australian Information Commissioner (OAIC) website if you want to find out more information about each principle.

The easiest way to get to the APPs is to search '**Australian Privacy Principles**' in your browser."

The following are summaries of key APPs that apply most to the work we do.

Open and transparent management of personal information

One of the ways we achieve this by publishing and maintaining our privacy policy on our website.

If a member of the public needs to read our Privacy Policy, you can guide them to it by asking them to go to our [fairwork.gov.au](https://www.fairwork.gov.au) website and searching 'privacy'.

Give someone the option to remain anonymous or use a pseudonym —

We must apply this option where it is practical for us to do so.

For example, we allow individuals the choice to make an anonymous report on our website.

Collection of solicited personal information —

Requires that we only collect personal information that is necessary for us to complete our work. If we need to collect sensitive information, we must get the individual's consent first in most circumstances.

Dealing with unsolicited personal information —

There may be circumstances where we receive unsolicited personal information that we didn't request.

The APP requires that we destroy or de identify that information in line with government archiving requirements as soon as practical.

Please follow the OFWO's processes on the 'Disposal of information' Intranet page before you destroy information.

Notification of the collection of personal information —

When we collect personal information, we provide collection statements that describe how we handle it.

For example, when we contact someone for evidence as part of an investigation and they provide their own personal information.

We must notify or make an individual aware of all personal information that we collect about them, whether we collect it directly or from a third party.

An example is how we describe a person's online privacy rights while using our website. We do this on our website's Privacy page.

Use or disclosure of personal information —

We can only use or disclose personal information for the primary purpose for which we collected it.

There are limited exemptions to this rule, such as where an individual has given us their consent for secondary use, or it is required to help enforcement bodies with their activities.

Quality of personal information —

We must maintain the personal information we use so that it is accurate, up-to-date and complete for the purpose we are using it for.

Security of personal information —

We must take reasonable steps to protect the personal information we hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.

We can take personal responsibility for this by keeping personal information in the systems designed to keep it protected.

Access to personal information —

This Principle requires that we must give an individual access to their own personal information if they ask us (in most circumstances).

It applies alongside the Freedom of Information Act 1982 which provides a right to request access to all government information.

Correction of personal information —

We must correct any incorrect personal information we use.

We can do this when we identify the personal information is incorrect, or when the individual requests we correct it.

CONTINUE

Identifying personal information



"CONSIDER

We collect various personal and sensitive personal information here at the OFWO.

Do you know how to identify personal information and sensitive personal information from other information?"

Below are definitions to help you:

Personal information

Personal information is information or an opinion, whether recorded in a material form or not, whether true or not, about an identified individual or an individual who is reasonably identifiable.

Sensitive personal information

Sensitive personal information is information that may have traditionally led to discrimination against the individual. The formal definition in the Privacy Act is a list of specific types of information.



“CONSIDER

Take a moment to think about the personal information you access or use in your role. How many different types can you think of?”

Select all the descriptions of information below describing **Personal information** which are not sensitive.

Business name

Comments recorded about a person’s sexual

- orientation
- Date of birth
- An OFWO employee's signature
- A description of a person's religious belief
- Photos of the inside of a workplace (without employees)
- A person's address
- A person's health information
- A photo of an individual's car

SUBMIT

Documents released by the Fair Work Ombudsman
Under the Freedom of Information

CONTINUE

Documents released by the Fair Work Ombudsman
Under the Freedom of Information

Applying the Privacy Principles in your role

After learning about the APPs and honing your skills in identifying personal information, you may have already developed a better understanding of how you can help us meet our privacy requirements.

The following are 5 examples of role specific behaviours that we must develop to maintain our privacy requirements.

Keep personal information secure

You have probably heard these requirements many times. There is a reason for it! The following behaviours are foundational to maintaining privacy:

- Keep personal information in the systems or secure containers designed to store it in.
- Maintain a clear desk and screen.
- Identify sensitive and security classified information by using applicable protective markings.
- Restrict access to personal information to a need-to-know basis.

Know what information we shouldn't collect

Our Privacy Policy is available from our Intranet and is available to the public through our website. It tells us that we should not collect the following:

- Tax File Numbers, in most circumstances.
- Covert recordings.
- Health information.

If we receive this as unsolicited information, we must take steps to either de-identify it or destroy it. If you are unsure, please contact your friendly Privacy Officer for advice.

Notify people when we collect their personal information —

We need to explain the following when we collect personal information directly or from a third party:

- who we are where it is not clear we work for the OFWO
- whether we are required to collect it by law
- why we are collecting it
- who we share it with.

We can do this verbally or in writing.

Check, double check and triple check – just to make sure! —

Many of the privacy breaches we investigate are due to human error. If you are sharing information, you must take the appropriate steps to make sure you are only sharing with the people that you need to share with, for example:

- If you are sending an email that contains personal information, make sure you check the recipients before you send.
- If you are sharing personal information using Microsoft 365 tools, make sure you check the share settings. The default settings are not always appropriate.

Know how to access our Privacy Policy —

You can access our Privacy Policy simply by searching 'privacy' on our Intranet.

Our Privacy Intranet page summarises our privacy requirements here in the OFWO and contains links to our policy documents and external links web pages like the Australian Privacy Principles.

Our customers can find our Privacy Policy on our fairwork.gov.au website. If you need to guide them, it is as simple as asking them to search 'Privacy' from our website's search function.

Our Privacy Policy explains the types of personal information we collect and the sources we collect it from. It explains how we use it, store it and for how long we need to keep it.

Please practice accessing our privacy information through the Intranet and our website. This will increase your confidence when you need to access it next.

Watch the video below to find out how you can protect personal information when using email (3:35)

View video transcript:



How you can protect personal information when using email - video transcript.pdf

139.1 KB



TASK

Search for the **Privacy Policy** on the Intranet

INTRANET

Search for the **Privacy Policy** on the FWO website

FWO WEBSITE

CONTINUE

Documents released by the Fair Work Ombudsman
Under the Freedom of Information

Privacy breaches

A person looking at a computer screen.

A privacy breach can range from simply emailing someone's personal information to the wrong recipient, through to large scale data breaches.

In June 2023, the OFWO was caught up in a data breach where Russian hackers stole data from a law firm that provides us with legal services. Many of our customers and our own staff had their personal information or work information stolen and published on the dark web.

This was a good example of how important it is for every one of us to stay vigilant, follow our security procedures and be aware of the security threats we face.

What to do if you identify a privacy breach

If you suspect you have caused a privacy breach or have identified an existing breach, it may be tempting to 'fix it' and move on. Instead, please report the breach via the Security and Privacy Incident Report (SETIR) form, and access and follow the OFWO's Privacy Breach Guide straight away.

Our Privacy Breach Guide provides general privacy information and describes the 5 steps you need to follow in a privacy breach, which are:

1

Preliminary assessment and reporting

- 2 **Internal escalation and consultation**
- 3 **Contain the breach**
- 4 **Consider notification to affected individuals and others**
- 5 **Preventing future breaches**

TASK

1. Search for the **Privacy Breach Guide** via the Intranet.
2. Search for the **Security and Privacy Incident Report (SETIR)** form in the FWO Employee Centre via the Intranet.

INTRANET

CONTINUE

Documents released by the Fair Work Ombudsman
Under the Freedom of Information

Lesson 7 of 10

Privacy knowledge check

Privacy is...

(Select all that apply)

- a human right
- making sure the government doesn't share information
- the right to be left alone
- controlling your identity
- having something to hide
- using a password manager

SUBMIT

Based on what you have learnt, select the sensitive personal information from the following:

(Select all that apply)

-
- Age
 - Sexual orientation
 - Religious beliefs
 - Political opinions
 - A person's address

SUBMIT

Select the correct ways to use personal information from the following:

(Select all that apply)

- Allow individuals using our website to stay anonymous.
- Email case information to your personal email so you can work on it at home from your personal computer.
- Collect sensitive personal information from all employees when conducting a workplace inspection.
- Provide images of people and their formal documents to the Australian Federal Police in a suspected Human Trafficking case.
- Access internal WHS systems to find out why your coworker is limping.

SUBMIT

Which of the following behaviours are essential for you to develop to keep personal information secure?

(select all that apply)

- Restrict access to personal information to a need-to-know basis.
- Maintain a clear desk and screen.
- Share it with your manager only
- Use applicable protective markings
- Save it in a shared Docbank folder that only your team can access.
- Keep it in specially designed systems or secure containers

SUBMIT

What are the first actions you should take if you identify a privacy breach?

- Cover it up – no-one gets hurt if no one knows about it.
- Add it to your follow up list for tomorrow morning when you have spare time to investigate.
- Go to the 'Privacy breach' Intranet page to access the Privacy Breach Guide for instructions and the SETIR form to report it.
- Call you manager and ask for help. Only managers handle privacy breaches.
- Put the details into your Microsoft Teams general chat to find out who is responsible.

SUBMIT

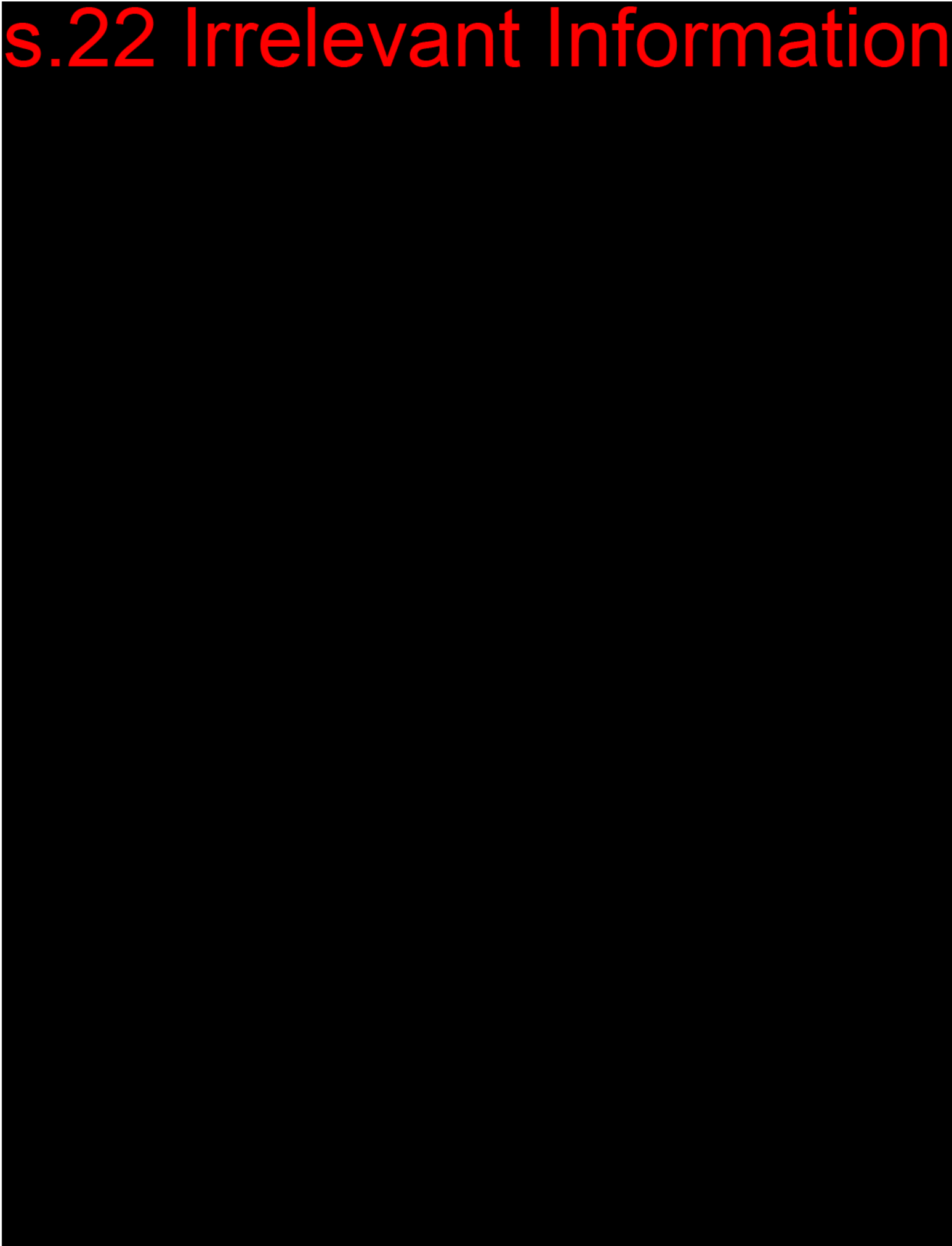
CONTINUE

Documents released by the Fair Work Ombudsman
Under the Freedom of Information

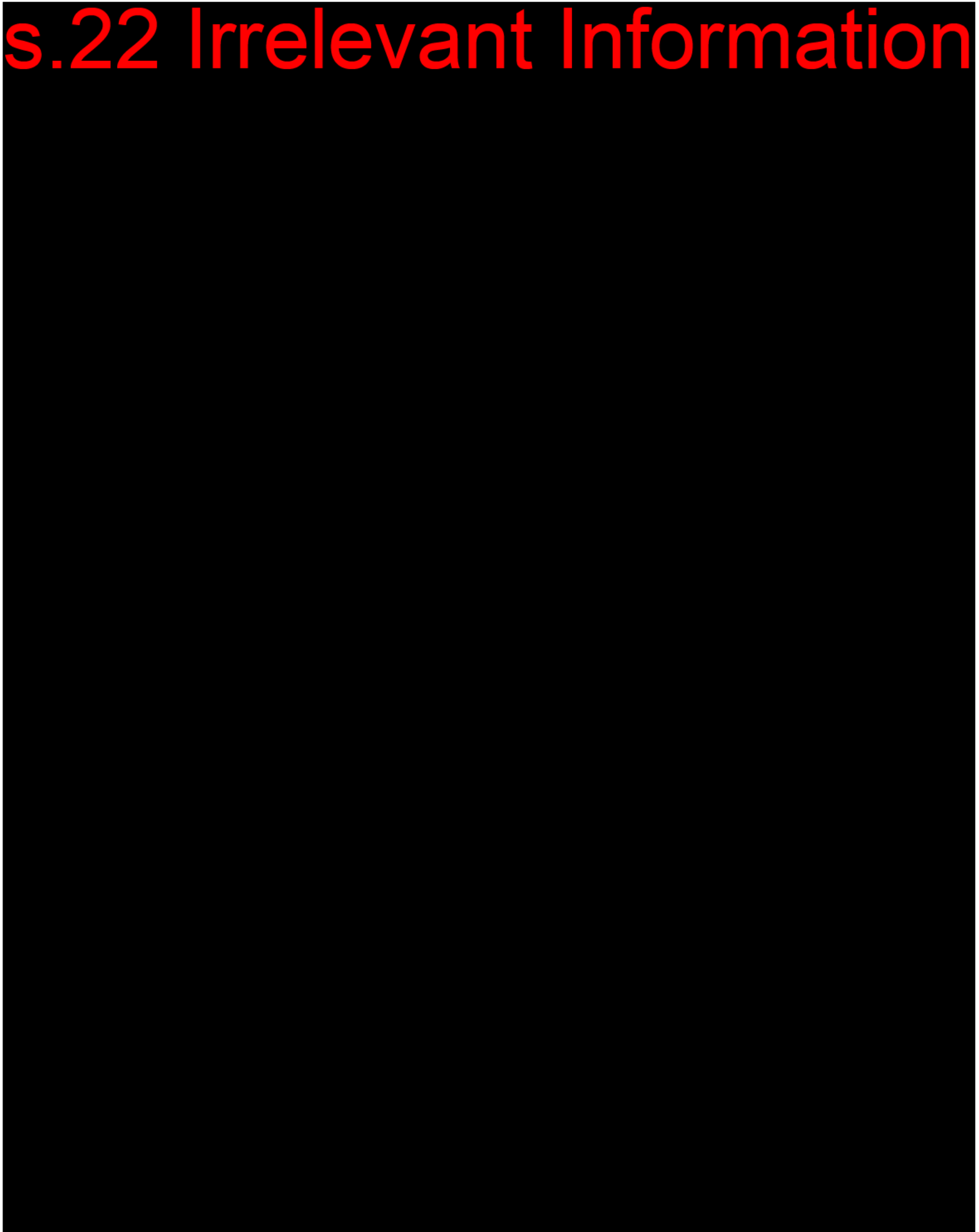
s.22 Irrelevant Information



s.22 Irrelevant Information



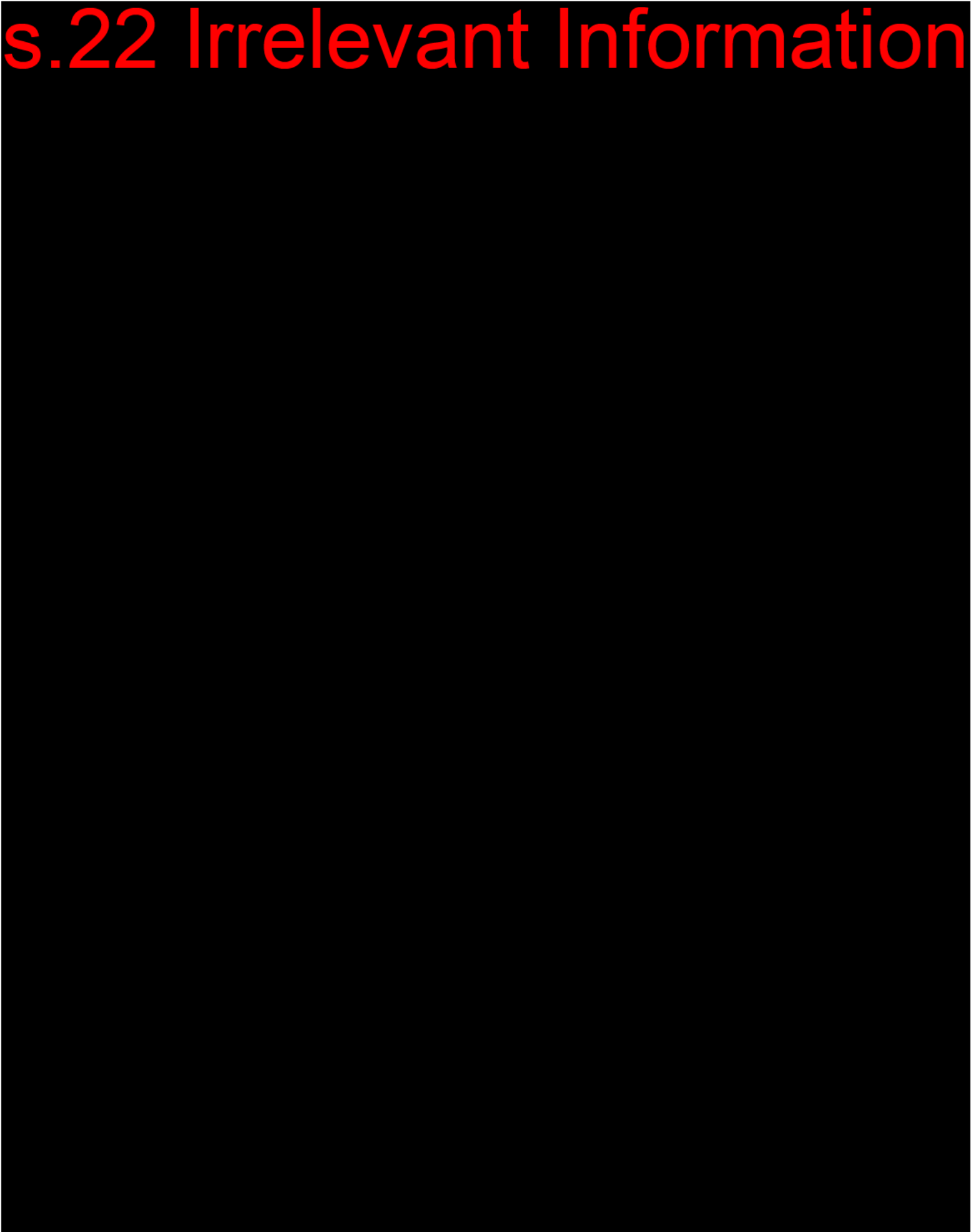
s.22 Irrelevant Information



s.22 Irrelevant Information



s.22 Irrelevant Information



s.22 Irrelevant Information



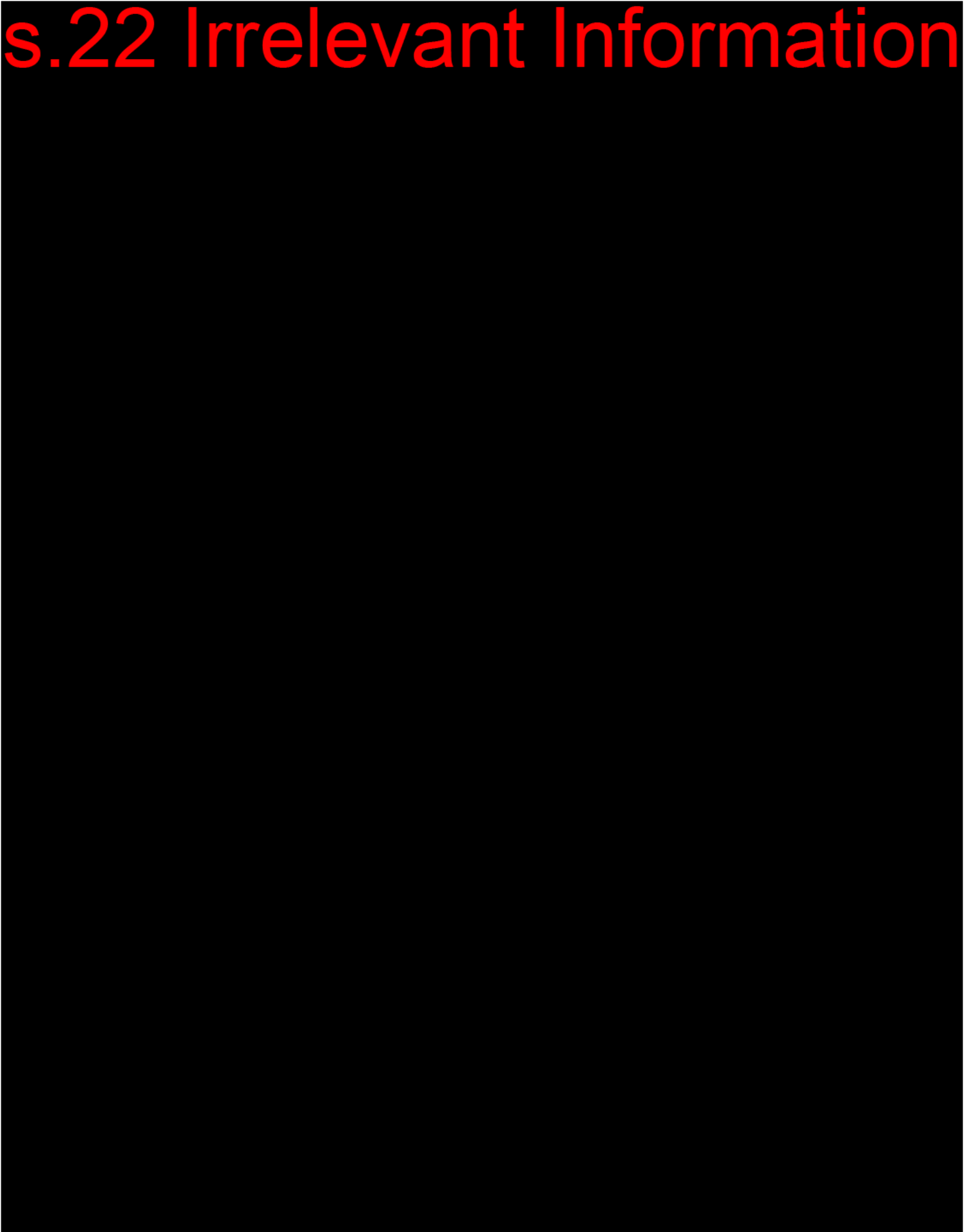
s.22 Irrelevant Information



s.22 Irrelevant Information

Documents released by the Fair Work Ombudsman
Under the Freedom of Information

s.22 Irrelevant Information

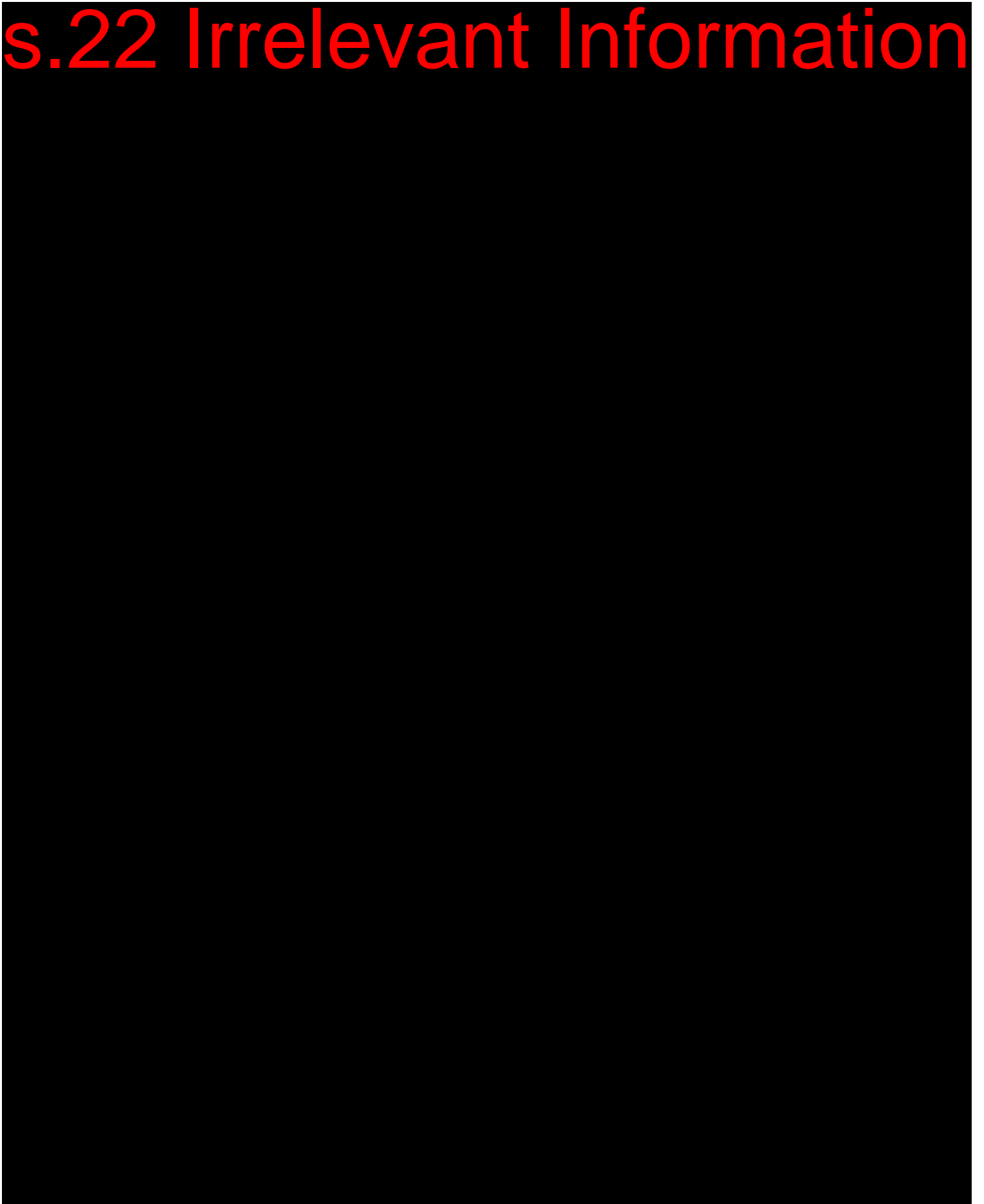


s.22 Irrelevant Information

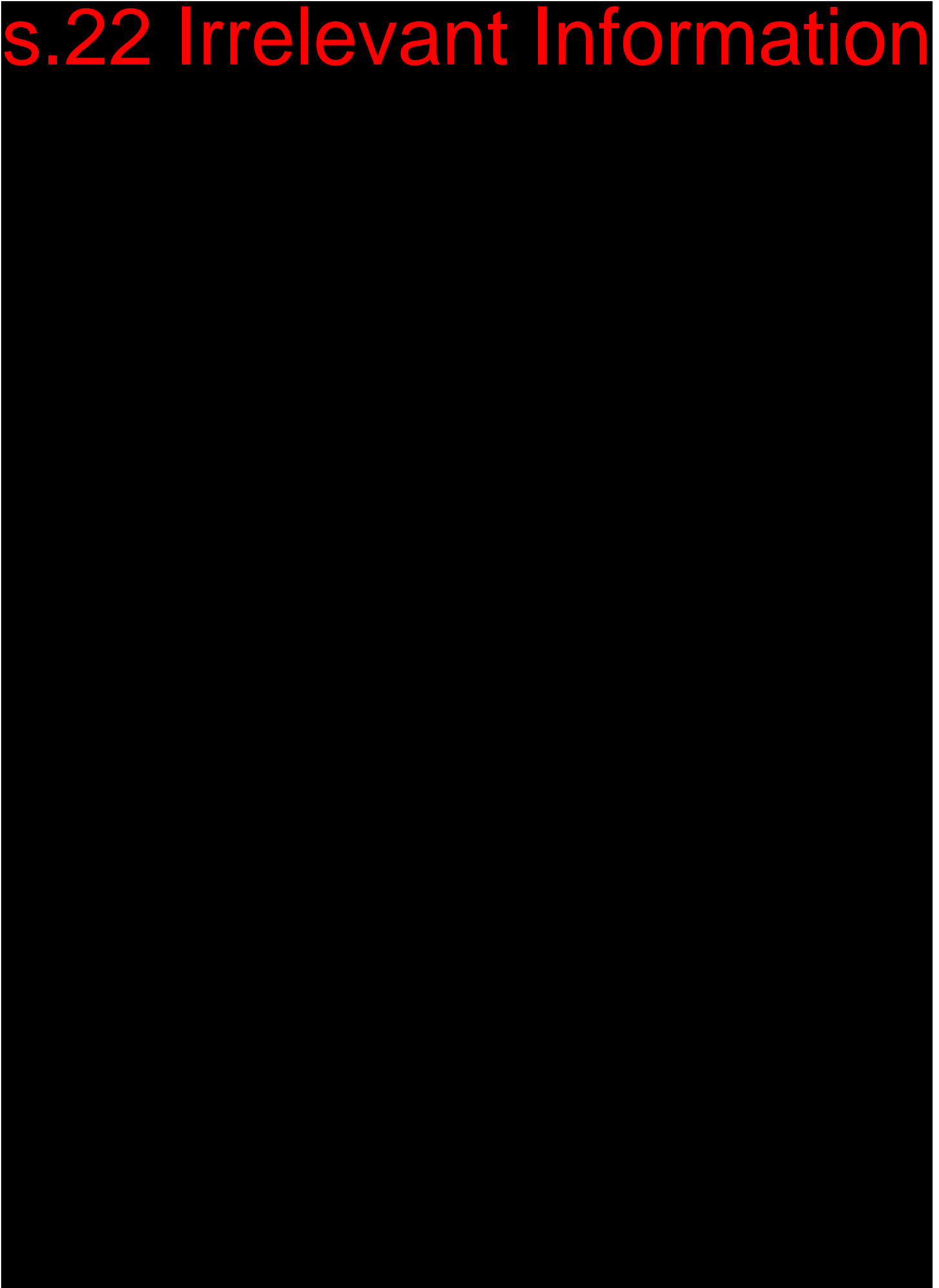


Documents released by the Fair Work Ombudsman
Under the Freedom of Information

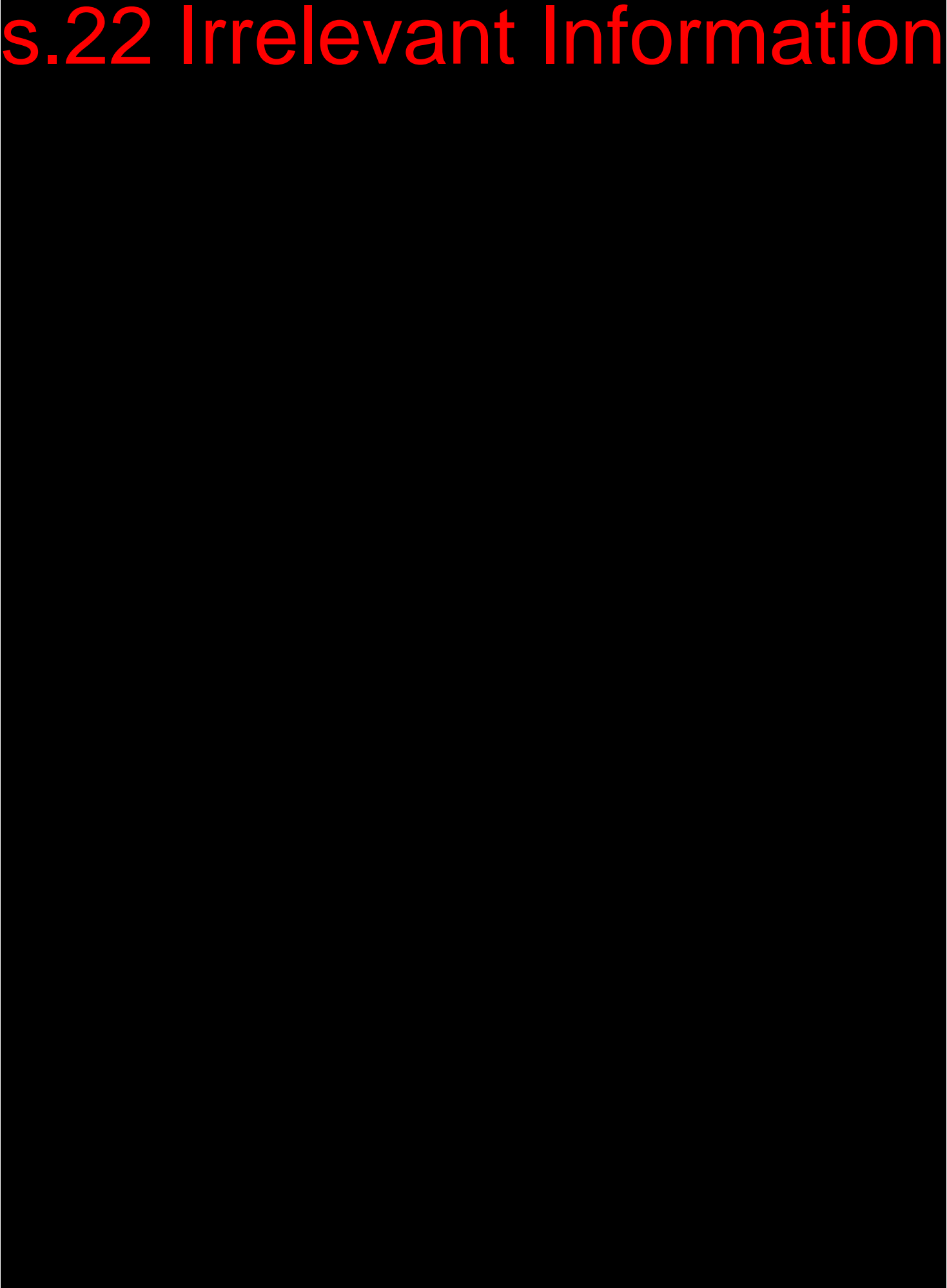
s.22 Irrelevant Information



s.22 Irrelevant Information



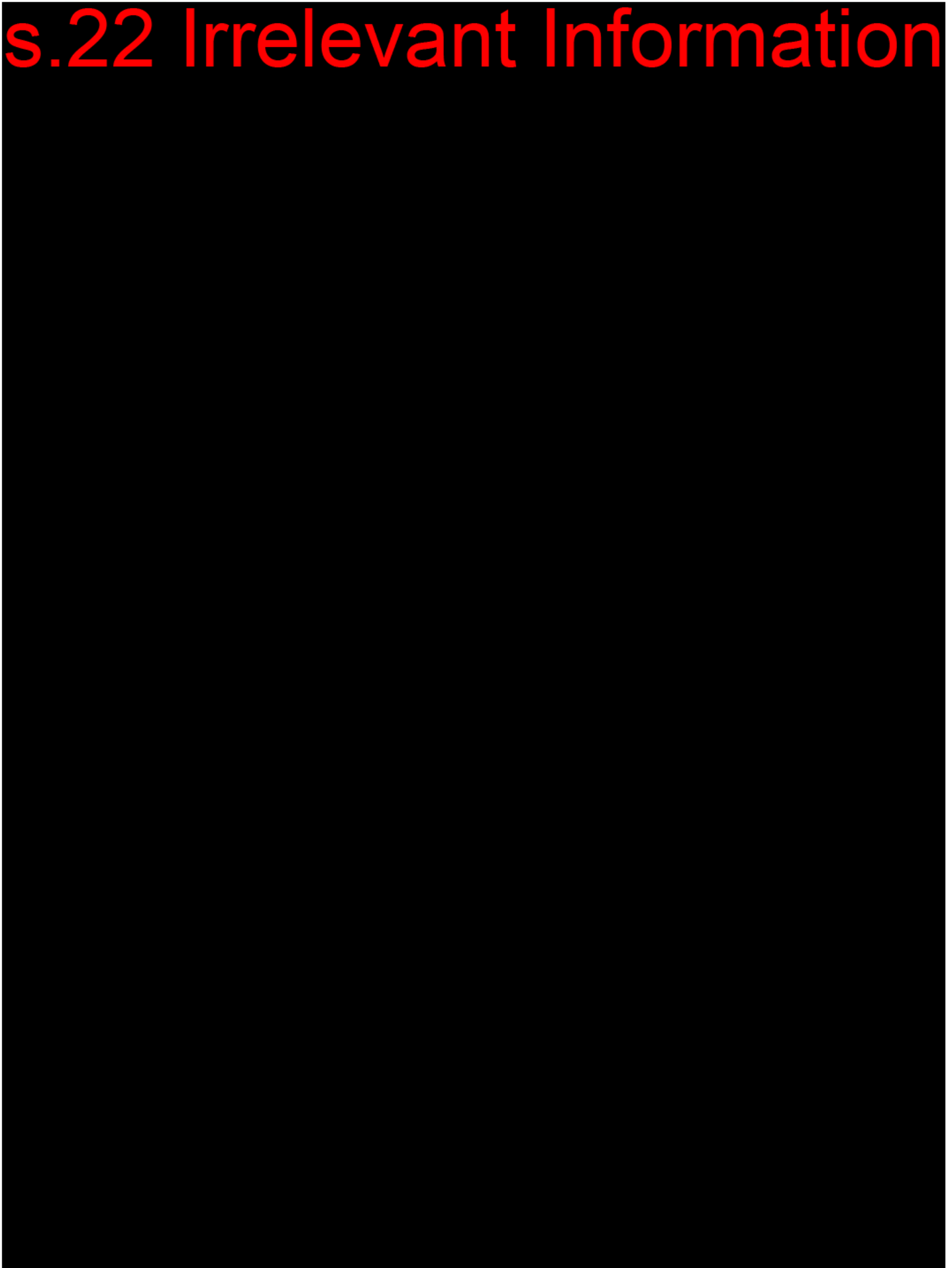
s.22 Irrelevant Information



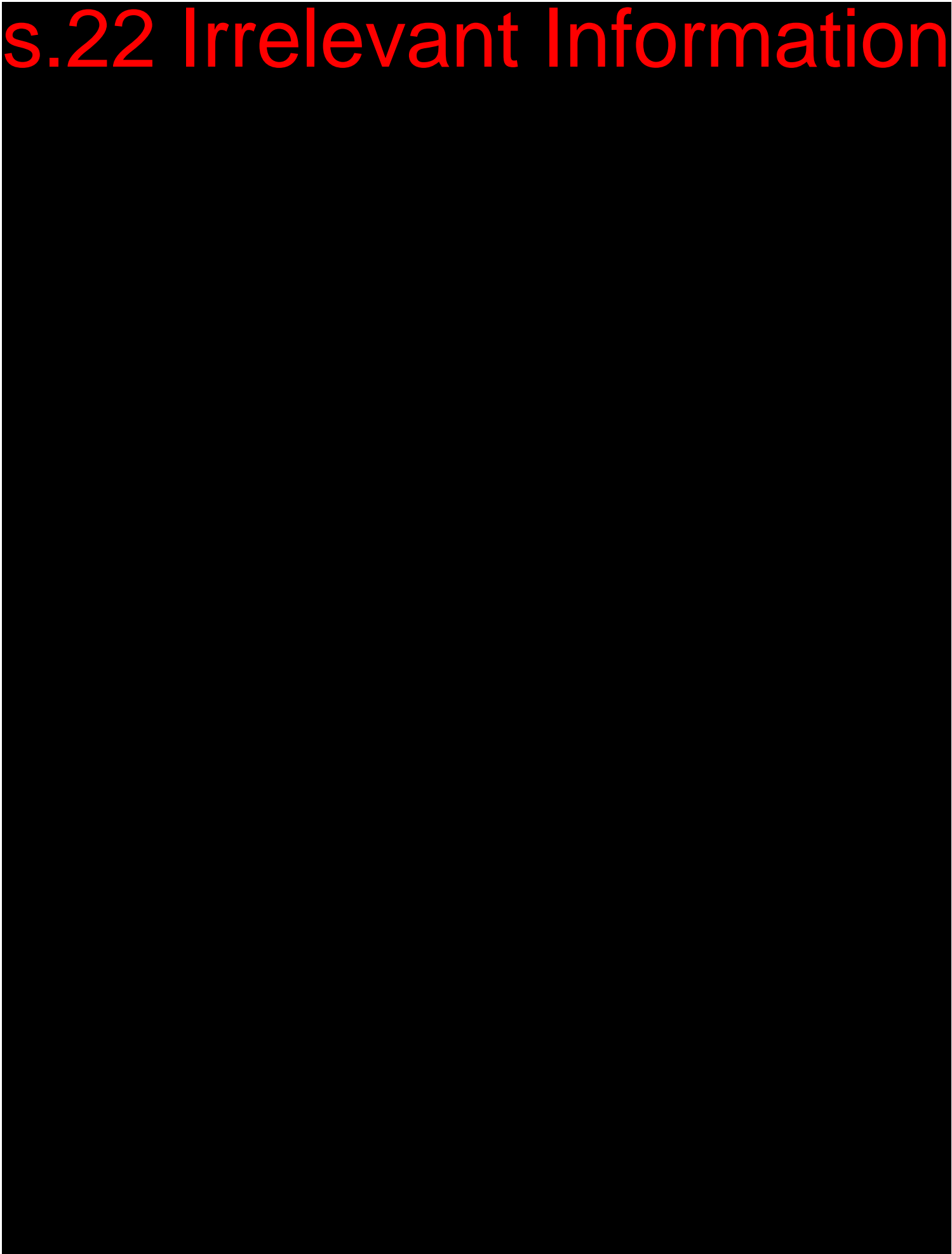
s.22 Irrelevant Information



s.22 Irrelevant Information



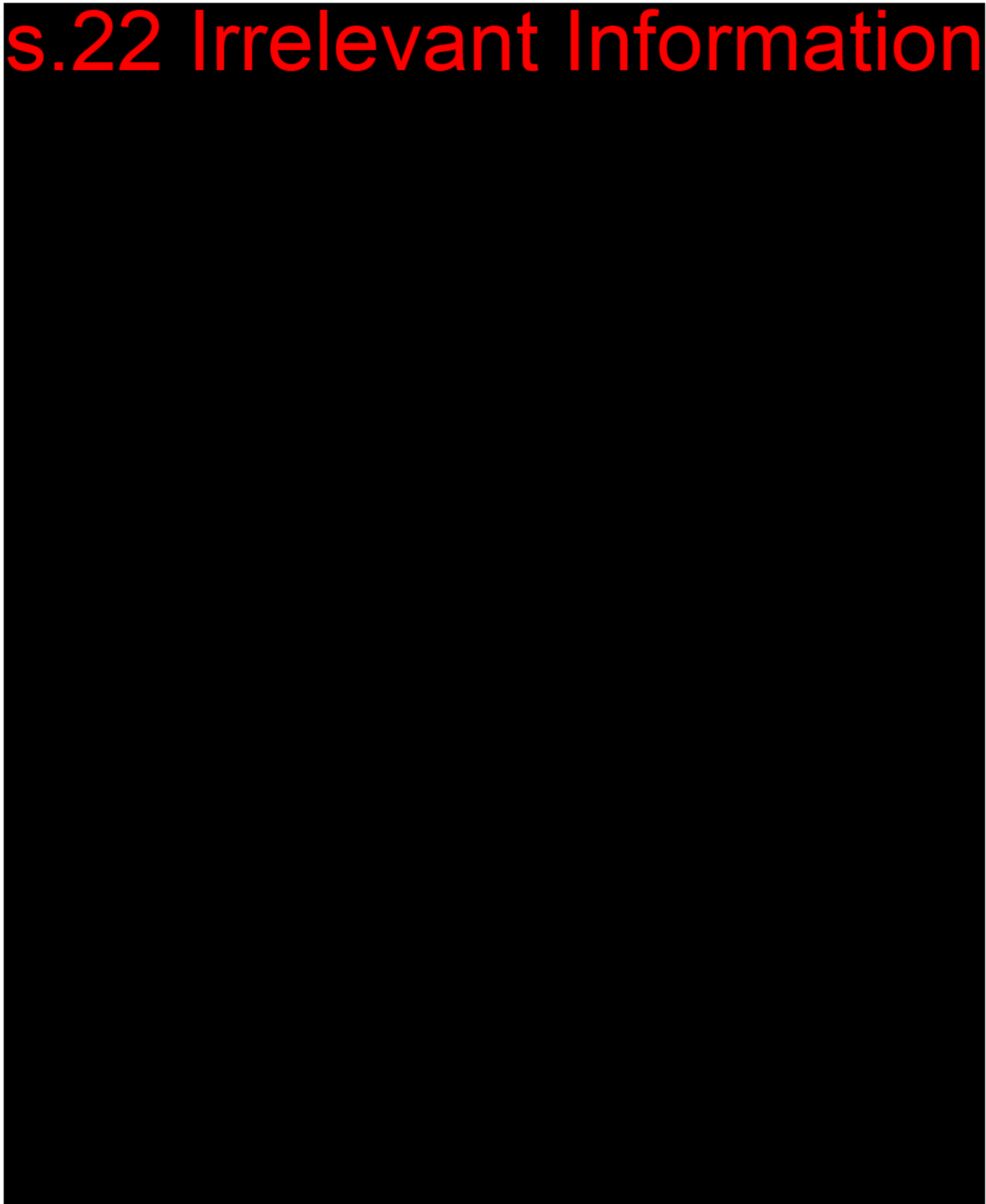
s.22 Irrelevant Information



s.22 Irrelevant Information

Documents released by the Fair Work Ombudsman
Under the Freedom of Information

s.22 Irrelevant Information



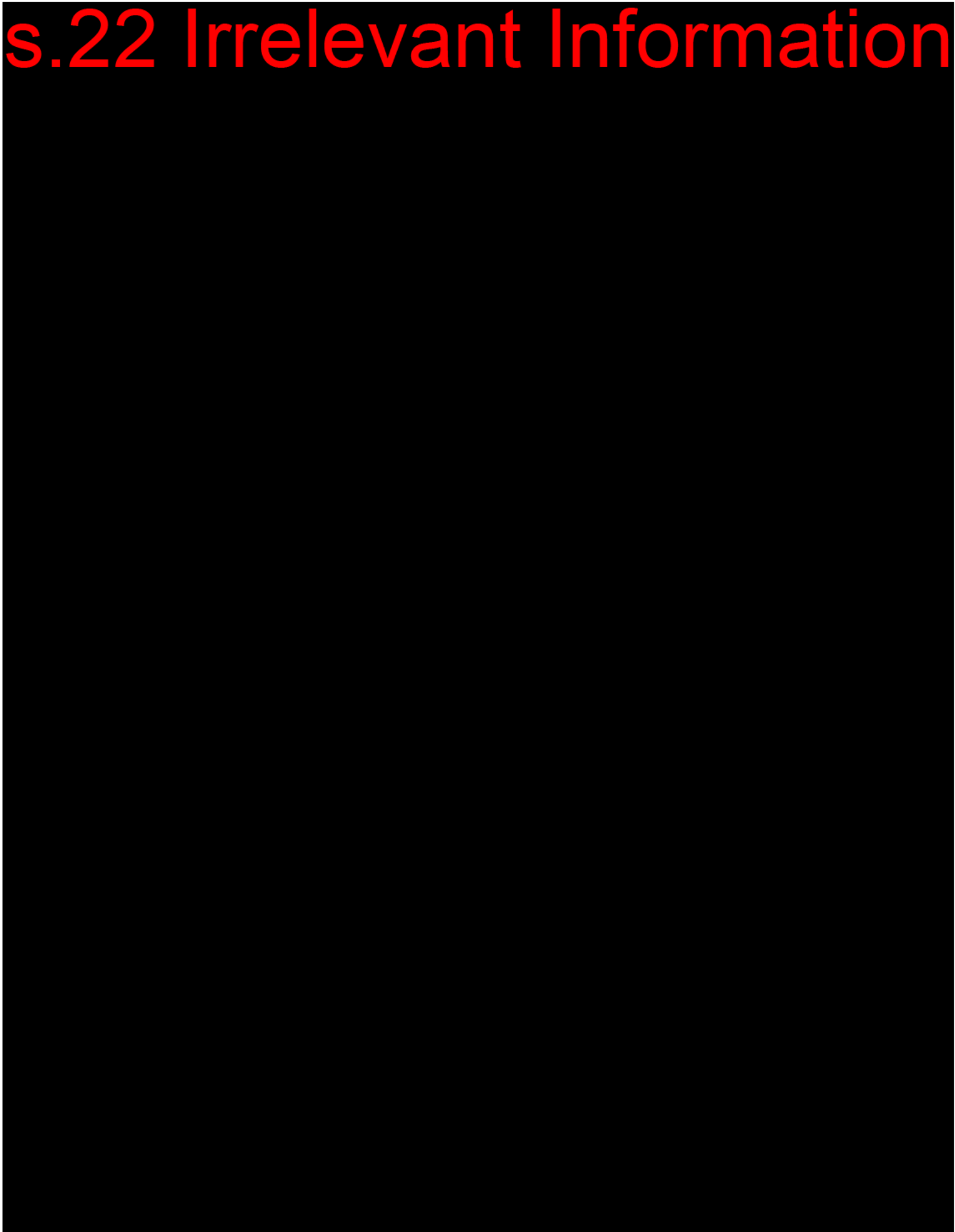
s.22 Irrelevant Information



s.22 Irrelevant Information



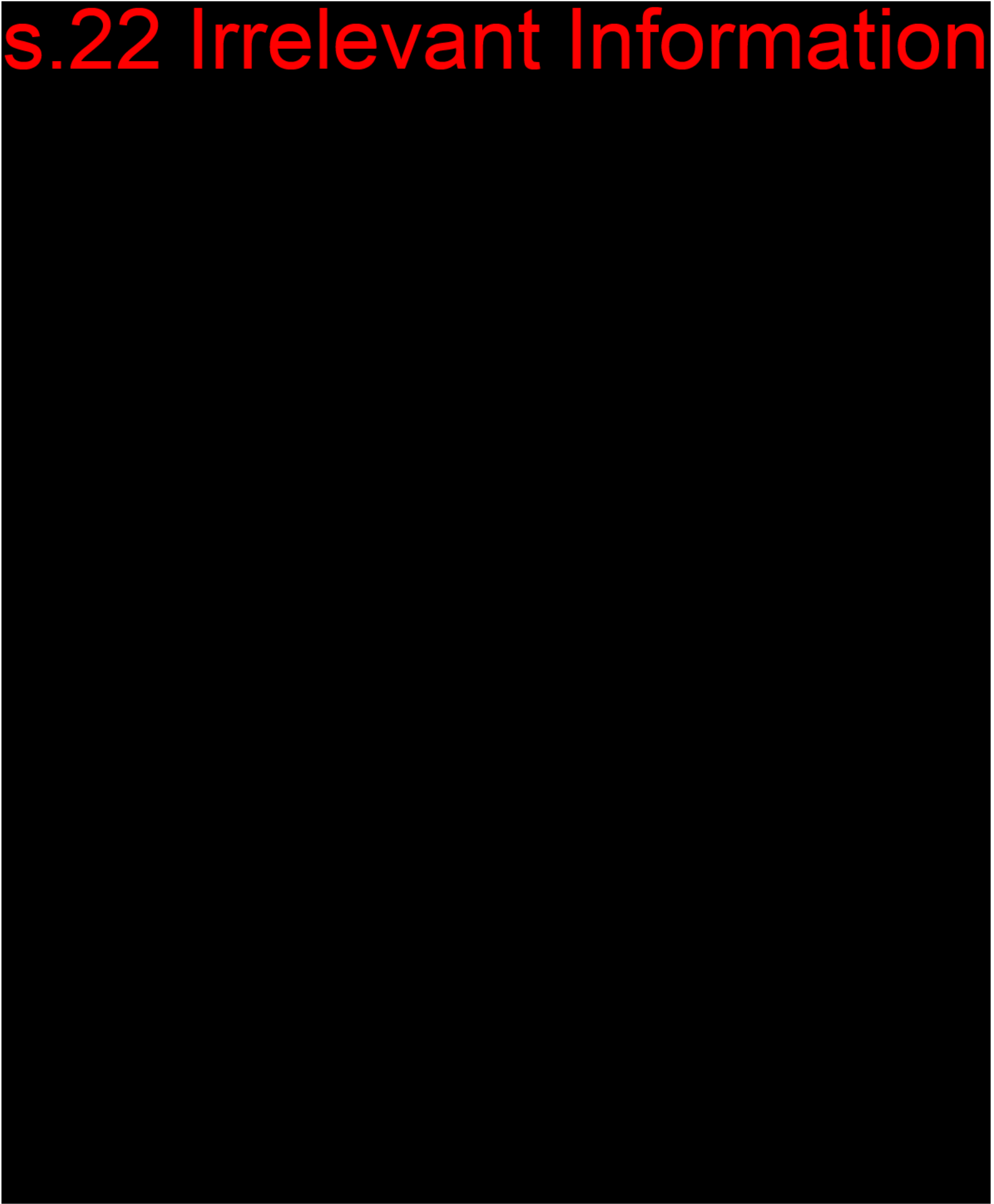
s.22 Irrelevant Information



s.22 Irrelevant Information

Documents released by the Fair Work Ombudsman
Under the Freedom of Information

s.22 Irrelevant Information





Australian Government

PRIVACY AWARENESS

Government agencies are committed to ensuring personnel receive adequate training and information on the Australian Privacy Principles (APPs) and other requirements under Australian privacy law. The Privacy Awareness eLearning program describes the APPs and related key concepts under the Privacy Act which govern how personal information is collected, used, disclosed and managed.

This program contains seven topics (with a quiz at the end of each) and is required training for all new employees and as an annual refresher for staff who have access to personal information in the course of performing their duties.

Documents released by the Fair Work Ombudsman
Under the Freedom of Information

Table of Contents

Topic 1 - Introduction to Australian Privacy Law.....	4
The Privacy Act.....	4
Powers of the Commissioner	4
Personal Information.....	5
Australian Privacy Principles	5
Australian Privacy Principles - a summary for APP entities.....	5
Privacy breaches	7
Example of privacy breaches	7
Topic 1 - Knowledge check.....	7
Key points to remember	9
Summary.....	9
Topic 2 – Open and transparent management of personal information.....	9
APP 1 - Open and transparent management of personal information.....	9
APP 2 - Anonymity and pseudonymity	10
Scenarios.....	10
Key points to remember	11
Summary.....	11
Topic 3 – Collection of personal information.....	11
Consent.....	12
Definitions.....	12
Consent Cont.....	14
APP 3 - Collection of solicited personal information	15
Identifying the functions or activities of an APP entity	15
APP 4 - Collection of unsolicited personal information	17
APP 5 - Notification of the collection of personal information	17
Privacy notices	17
Scenarios.....	18
Key Points to remember	19
Summary.....	19
Topic 4 – Dealing with personal information.....	20
APP 6 - Use or disclosure of personal information.....	20
APP 7 - Direct marketing.....	21
APP 8 - Cross-border disclosure of personal information.....	21
APP 9 - Adoption, use or disclosure of government related identifiers.....	21

Scenarios.....22

Key points to remember23

Summary.....24

Topic 5 – Integrity of personal information24

 APP 10 - Quality of personal information24

 APP 11 - Security of personal information.....24

 Scenario25

 Key points to remember25

 Summary.....25

Topic 6 – Access to, and correction of, personal information26

 Learning Objectives26

 APP 12 - Access to personal information.....26

 APP 13 - Correction of personal information26

 Scenarios.....27

 Key points to remember27

 Summary.....28

Topic 7 – Code Requirements28

 Learning Objectives28

 Australian Government Agencies Privacy Code28

 Privacy Impact Assessments (PIA)29

 Topic 7 - Knowledge check.....30

 Key points to remember30

 Summary.....31

Topic 8 – Notifiable Data Breaches scheme.....31

 Learning Objectives31

 eligible data breaches.....31

 Suspected Eligible Data Breaches.....32

 Scenarios.....32

 Key points to remember33

 Summary.....33

Module complete.....33

TOPIC 1 - INTRODUCTION TO AUSTRALIAN PRIVACY LAW

Overview

This topic provides information regarding the *Privacy Act 1988* (Privacy Act), the Australian Privacy Principles and what 'personal' and 'sensitive information' is.

Objectives

By the end of this topic, you should be able to:

- describe what 'personal information' and 'sensitive information' is
- outline the powers of the Australian Information Commissioner
- summarise the APPs.

[Return to Table of Contents](#)

THE PRIVACY ACT

The *Privacy Act 1988* (Privacy Act) protects the personal information that government and those private sector organisations covered by the Privacy Act (entities) collect about individuals.

The Privacy Act defines personal information and sets down minimum standards for the management of personal information by entities, set out in the Australian Privacy Principles (APPs).

The Privacy Act gives the Australian Information Commissioner (Commissioner) broad powers to assist and require entities to adopt policies and practices for handling personal information which comply with the Privacy Act and the APPs.

The APPs regulate how entities collect, store, provide access to, use and disclose the personal information of all individuals, including customers and staff. They also allow individuals to access their own information, and request correction if the information is incorrect.

Compliance with the APPs is a legal requirement.

The areas of privacy regulated by the Privacy Act is just one aspect of information management. Confidentiality, secrecy, intellectual property and freedom of information are not regulated by the Privacy Act.

[Return to Table of Contents](#)

POWERS OF THE COMMISSIONER

The Office of the Australian Information Commissioner (OAIC) has responsibility for regulating and providing advice on the operation of the Privacy Act. The powers of the Commissioner include powers:

- to work with entities covered by the Privacy Act to facilitate compliance and best practice, such as directing an agency to undertake a Privacy Impact Assessment (PIA), directing an entity to notify affected individuals and inform the Commissioner about 'eligible privacy breaches' and conducting an assessment of whether personal information is being handled lawfully
- to investigate potential privacy breaches on the Commissioner's own motion or in response to complaints (including by requiring a person to produce information or a document, or to attend and answer questions under oath), make determinations about whether there has been a breach and require entities to take action in response, including paying financial compensation
- to take various enforcement actions, including accepting an enforceable undertaking and bringing proceedings to enforce it, bringing court proceedings to enforce a determination, reporting to the Minister and applying to a court for a civil penalty (up to \$1.7 million) for significant and/or repeated breaches of privacy.

[Return to Table of Contents](#)

PERSONAL INFORMATION

Personal information is defined in the Privacy Act to mean information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, or recorded in a material form or not.

Sensitive information is a subset of personal information. It includes information or opinions about racial or ethnic origin, political opinions, membership of political, professional or trade associations or trade unions, religious beliefs or affiliations, philosophical beliefs, sexual orientation or practices and criminal records. Sensitive information also includes health and any other genetic information about an individual, as well as biometric information and templates.

Health information includes information or an opinion about the health, illness, disability or injury (at any time) of an individual as well as information regarding health services provided or to be provided to an individual and a person's expressed wishes about future provision of health services.

Biometrics is the identification of people based on their unique traits or characteristics. Biometric information refers to measurements of human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. Biometric templates are a digital representation of an individual's distinct characteristics, representing information taken from a biometric sample. It is the biometric template that is actually compared in a biometric recognition system.

Many agencies will also encounter other types of information, for example, 'protected information' under the *Social Security Act 1991* or agencies may have access to tax file numbers. Additional protections apply to the use of this information and these are dealt with separately in Social Security and Taxation legislation, respectively.

What is considered personal information can change depending on the context of the situation, including (for example) number of people in a relevant group and what additional information may be available from other sources. For instance, an individual or small number of people with rare or very unusual characteristics from the same small regional town may be identifiable if their unusual characteristics and the town they are from is disclosed/known.

Video: <https://www.oaic.gov.au/updates/videos/privacy-in-the-australian-public-service/>

[Return to Table of Contents](#)

AUSTRALIAN PRIVACY PRINCIPLES

The Australian Privacy Principles (APPs) regulate the handling of personal information by both Australian government agencies and those businesses covered by the Privacy Act.

There are 13 APPs structured to reflect the information life cycle, from ensuring transparency in information collection, through to use and disclosure, quality and security, access and correction.

Under the APPs, private sector organisations and government agencies are collectively 'APP entities' or 'entities'. Where an APP only applies to government agencies, they are referred to as 'agencies' and where an APP only applies to private sector organisations, they are referred to as 'organisations'.

[Return to Table of Contents](#)

AUSTRALIAN PRIVACY PRINCIPLES - A SUMMARY FOR APP ENTITIES

APP 1 — Open and transparent management of personal information

Ensures APP entities manage personal information in an open and transparent way, including having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. Higher standards apply to the collection of 'sensitive' information.

APP 4 — Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information

Outlines an APP entity's obligations when an individual requests access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals where it is inaccurate, out of date, incomplete, irrelevant or misleading, having regard to the purpose for which the information is held.

[Return to Table of Contents](#)

PRIVACY BREACHES

An interference with privacy occurs where an act or practice of an entity breaches one of the APPs.

Departments or agencies are responsible for ensuring practices and procedures comply with the APPs.

Where a potential breach of privacy has been identified, you need to report the matter to your supervisor and your agency's Privacy Officer as soon as practicable.

Where a privacy breach is an **eligible data breach**, the Office of the Australian Information Commissioner (OAIC) and the affected individual(s) must be notified.

An '**eligible data breach**' is an unauthorised access to or disclosure of, or loss of personal information that is likely to result in serious harm to the affected individuals.

Information regarding eligible data breaches is discussed in more detail in Topic 8.

Failure to report a privacy incident in a timely manner can result in serious consequences such as the risk of harm to the person whose privacy has been breached, adverse media or Parliamentary attention.

Under the Privacy Act there are no penalties for the individual who breaches privacy, however, a staff member may be subject to disciplinary action under the *Public Service Act 1999*.

[Return to Table of Contents](#)

EXAMPLE OF PRIVACY BREACHES

Examples of privacy incidents include, but are not limited to:

- "I have left personal information on my desk unsecured at the end of the day".
- "I disclosed a customer's personal information (address, phone number and employer) to another party".
- "I collected a letter from the printer, but accidentally picked up a different customer's statement and posted it with the customer letter".
- "I left customer details in a public place while transporting them".
- "I accidentally sent an email to a group of people but I used the 'to' field instead of the 'bcc', so everyone who received it can see everyone else's email addresses".
- "I sent an email containing personal information to the wrong recipient when Outlook AutoCompleted the email address".
- "I accidentally published a dataset online which contains personal information".

[Return to Table of Contents](#)

TOPIC 1 - KNOWLEDGE CHECK

To test your knowledge of the information presented in this topic, answer the following questions.

QUESTION 1

Select the correct answer to finish the sentence.

The Privacy Act...

- a. Protects government agencies from prosecution if they mishandle personal information.
- b. Protects the personal information that government and businesses collect about individuals.
- c. Regulates confidentiality, secrecy, intellectual property and freedom of information.

Enter your answer(s):

QUESTION 2

Select the correct answer.

Who needs to comply with the APPs?

- a. All legal entities in Australia.
- b. Agencies can opt in or out as they choose.
- c. Compliance with the APPs is a legal requirement for APP entities that are agencies including Australian Government agencies and some private sector organisations as defined in the *Privacy Act 1988*.

Enter your answer(s):

QUESTION 3

Select the correct answer.

Who has responsibility for regulating and providing advice on the operation of the Privacy Act?

- a. The Federal or State Minister responsible for each Government agency.
- b. The Office of the Australian Information Commissioner (OAIC).
- c. No one is responsible, each Government agency regulates the Privacy Act themselves.

Enter your answer(s):

QUESTION 4

Select the correct answer.

Who is responsible for ensuring practices and procedures comply with the APPs?

- a. Departments or agencies.
- b. The Office of the Australian Information Commissioner (OAIC).
- c. Individuals who deal with the Australian Government.

Enter your answer(s):

QUESTION 5

Select the correct answer.

Which of the following is 'personal information'?

- a. A person's name.
- b. A person's phone number.
- c. A person's email address.
- d. A person's photograph.
- e. All of the above.

Enter your answer(s):

[Return to Table of Contents](#)

KEY POINTS TO REMEMBER

- Compliance with the APPs is a legal requirement.
- The Office of the Australian Information Commissioner (OAIC) is responsible for regulating compliance with the Privacy Act.
- Personal information is information or an opinion about an identified person, or a person who is reasonably identifiable. The information or opinion may, or may not, be true and may, or may not, be recorded in a material form.
- We must consider sensitive information, a subset of personal information, which includes certain types of information (for example, health information) listed in the Privacy Act.
- The APPs apply to 'APP entities' that are 'agencies' (including our department) or private sector 'organisations' as defined in the Privacy Act.
- Potential breaches of privacy need to be reported as soon as practicable to your supervisor and the agency's Privacy Officer.

[Return to Table of Contents](#)

SUMMARY

Great! You should be able to:

- describe what personal information and sensitive information is
- summarise the APPs
- outline the powers for the Australian Information Commissioner.

Click the **Additional Links** button below, to further explore this module:

- [Office of the Australian Information Commissioner](#)
- [Privacy Act 1988](#)

[Return to Table of Contents](#)

TOPIC 2 – OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION

Overview

This topic provides information on open and transparent management of personal information.

Objectives

By the end of this topic, you should be able to:

- summarise APP 1 and APP 2
- identify work situations where APP 1 and/or APP 2 will apply.

[Return to Table of Contents](#)

APP 1 - OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION

APP 1 outlines the requirement for APP entities to have a clearly expressed and up to date privacy policy. The privacy policy must set out:

- the kinds of personal information we collect and hold
- how we collect and hold personal information
- the reason we collect, hold, use and disclose this information
- how people access and amend their information.

Entities must take reasonable steps to implement processes that will ensure we comply with the APPs and enable us to deal with enquiries or complaints. Reasonable steps may include:

- training staff about our policies and procedures
- establishing procedures to receive and respond to complaints and enquiries
- establishing procedures to identify and manage privacy risks.

Note 1: The privacy policy must be made available free of charge and in an appropriate form. An appropriate form includes making it available on the entity's website.

If a person requests a copy of the privacy policy in a particular form (for example, printed) we must take reasonable steps to give the person a copy in that form.

Note 2: The policy will also need to outline whether personal information will be disclosed to overseas recipients, how a person can make privacy complaints, and how complaints will be dealt with.

[Return to Table of Contents](#)

APP 2 - ANONYMITY AND PSEUDONYMITY

APP 2 imposes obligations for APP entities to allow people to deal with us anonymously, or by using a pseudonym, if they want to, unless:

- the entity is required or authorised by or under an Australian law, or an order of a court/tribunal, to deal with people who have identified themselves
- it is impracticable for the entity to deal with people who have not identified themselves or used a pseudonym.

What amounts to 'impracticable' will depend on the circumstances. For example, where a person applies for a benefit to be paid to them, the service delivery agency cannot deal with that person without knowing their identity.

That agency will need to confirm who they are paying the benefit to, so will be unable to deal with the person anonymously on that particular matter.

[Return to Table of Contents](#)

SCENARIOS

SCENARIO QUESTION 1

Select one or more as appropriate (please note there may be more than one correct answer).

Jane, a customer of the department, is filling out a form that requests her personal information. Jane wants to know more about what the department will do with her personal information.

What can Jane do?

- Read the privacy notice on the form, and then read the privacy policy on the internet.
- Contact the department and ask for a printed copy of the privacy policy.
- Nothing, as the department can do whatever it wants with Jane's personal information.

Enter your answer(s):

SCENARIO QUESTION 2:

Select one or more as appropriate (please note there may be more than one correct answer).

Mary wants to know what services or assistance the department can provide to her, but she doesn't want to be identified because her ex-husband works for the department.

What can Mary do?

- The department will not deal with Mary, either face-to-face or over the phone, unless she identifies herself.
- Mary can visit the department in person and ask for general information about the department's services without giving her name.
- Mary can call the department and ask for general information about the department's services without giving her name.

Enter your answer(s):

KEY POINTS TO REMEMBER

APP 1 - OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION

- We must have a clear and current privacy policy that sets out the kinds of personal information we collect and hold, and how we manage that information.
- The policy must be free of charge and in an appropriate form.
- We must set up processes to ensure we comply with the APPs and deal appropriately with enquiries or complaints.

[Return to Table of Contents](#)

APP 2 - ANONYMITY AND PSEUDONYMITY

- We must allow people to deal with us anonymously or with a pseudonym if they want to, unless it is impracticable to do so, or identification is required by Australian law or an order of a court/tribunal.

[Return to Table of Contents](#)

SUMMARY

Great! You should be able to:

- summarise APP 1 and APP 2
- identify work situations where APP 1 and/or APP 2 will apply.

[Return to Table of Contents](#)

TOPIC 3 – COLLECTION OF PERSONAL INFORMATION

Overview

This topic provides information on the collection of personal information.

Objectives

At the end of this topic you should be able to:

- discuss the term 'consent'
- outline how to identify entity functions or activities
- discuss the term 'reasonably necessary'
- outline what a privacy notice is and why it is used

- summarise APP 3, APP 4 and APP 5
- identify work situations where APP 3, APP 4 and/or APP 5 will apply.

[Return to Table of Contents](#)

CONSENT

When consent is needed to collect, use or disclose information, the APP entity should implement procedures and systems to obtain and record consent.

There should be no doubt that consent has been given, either expressly or clearly implied from the conduct of the person.

Consent means **express consent** or **implied consent**. Four key elements of consent are:

- it must be provided **voluntarily**
- the individual must be adequately **informed** of what they are consenting to
- it must be **current and specific**
- the individual must have the **capacity** to understand and communicate their consent.

Note 1: Where a person cannot consent, they should be involved, as far as is practical, in any decision-making process. If possible, ensure privacy issues are discussed in a way that is understandable and comprehensible.

Note 2: The Privacy Act does not specify an age after which people can make their own privacy decisions. An APP entity will need to determine whether a young person has the capacity to consent on a case-by-case basis. As a general principle, a young person has capacity to consent when they have sufficient maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person.

[Return to Table of Contents](#)

DEFINITIONS

EXPRESS CONSENT

Express consent is given explicitly, either verbally or in writing, which could include a signature or a spoken statement to signify agreement.

[Return to Table of Contents](#)

IMPLIED CONSENT

Implied consent arises where consent may reasonably be inferred from the conduct of the person and the APP entity.

[Return to Table of Contents](#)

VOLUNTARY

Consent is voluntary if a person has a genuine opportunity to provide or withhold their consent. Consent is not voluntary where there is duress, coercion or extreme pressure.

Factors relevant to deciding whether consent is voluntary include:

- the alternatives open to the person, if they choose not to consent
- the seriousness of any consequences if a person refuses to consent

- any adverse consequences for family members or associates of the person if the person refuses to consent.

[Return to Table of Contents](#)

INFORMED

A person must be aware of the implications of providing or withholding consent. For example, whether the person is able to access a service if they do not consent to an APP entity collecting a specific piece of personal information.

An APP entity should give information directly to the person about how their personal information will be handled, in a way that the person understands.

The information should be written in plain English, without legal or industry jargon.

[Return to Table of Contents](#)

CURRENT AND SPECIFIC

An APP entity should seek consent from a person at the time it wants to collect, use or disclose that person's personal information. You should not seek a broader consent than is required for that purpose. For example, consent for undefined future uses, or consent to 'all legitimate uses or disclosures'.

A person may withdraw their consent at any time. If they do, an APP entity would no longer be able to rely on consent having been given when dealing with that person's personal information.

[Return to Table of Contents](#)

CAPACITY

A person must be able to understand the issues relating to the decision to consent. This includes the effect of giving or withholding consent, forming a view based on reasoned judgement and communicating their decision. An entity should not rely on any statement of consent given by a person if it is unsure they have the capacity to consent. Issues that could affect a person's ability to consent include:

- age
- physical (e.g. vision impairment which affects reading ability) or mental disability or impairment
- temporary incapacity
- limited understanding of English.

An entity should consider providing support to enable the person to exercise their capacity. If a person does not have capacity to consent and consent is required, an entity should consider who can act on the person's behalf. Options include:

- a guardian
- someone with an enduring power of attorney
- a person recognised by other relevant laws, such as a person's spouse, partner, carer, family member or close friend
- a person who has been nominated in writing by the person while they were capable of giving consent.

[Return to Table of Contents](#)

CONSENT CONT.

OPT OUT CONSENT MECHANISMS

It is unreliable to assume implied consent based on a person's failure to opt out. However, opt out consent models may be appropriate where the following factors are met:

- the option to opt out was clearly presented
- it is likely the person received and read the information about the proposed collection, use or disclosure, and the offer to opt out
- the person was aware of the implications of not opting out
- the choice to opt out is freely available and not bundled with other purposes
- opting out is easy to take up. That is, it involves little or no financial cost to, or effort from, the person
- the consequences of failing to opt out are not serious
- if the person opts out later, they are fully restored to the position they would have been in if they had opted out earlier.

[Return to Table of Contents](#)

IMPLIED CONSENT

Where consent may reasonably be inferred from the conduct of the individual and the APP entity.

It should not be assumed that a person has consented to collection, use or disclosure just because the collection, use or disclosure appears to benefit that person.

It should not be assumed that a person has given consent because they have not objected to a proposal to handle personal information in a particular way.

Implied consent may not be relied upon where there is reasonable doubt about the person's intention.

[Return to Table of Contents](#)

EXPRESS CONSENT

Express consent is given fully and clearly, either verbally or in writing. This could be a signature or a spoken statement to signify agreement.

An APP entity should seek express consent where it proposes to handle a person's sensitive information (unless one of the exceptions in APP 3.4 applies).

[Return to Table of Contents](#)

BUNDLED CONSENT

Bundled consent is where an individual is requested to agree to a wide range of collections, uses and disclosures at the same time. Not allowing the individual the ability to opt out of some of the collections, uses or disclosures of personal information within the bundle can undermine the voluntary nature of consent.

[Return to Table of Contents](#)

APP 3 - COLLECTION OF SOLICITED PERSONAL INFORMATION

APP 3 outlines when and how an entity may collect the personal and sensitive information it **solicits** from a person or another entity.

An entity '**solicits**' personal information if the entity requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included.

We can only collect personal information if it is reasonably necessary for, or directly related to, one or more of our functions or activities.

Collection of personal information must be by lawful and fair means. Personal information must be collected from the individual concerned unless:

- the individual consents to collection from someone other than the individual
- the agency is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual
- it is unreasonable or impracticable to do so or an exception applies.

The APPs impose more restrictive obligations when collecting sensitive information. Sensitive information can be collected:

- if the person consents and the information is reasonably necessary for, or directly related to, one of the entity's functions or activities
- if the collection is required or authorised by law
- in permitted general situations.

Some examples of permitted general situations are:

- where collection, use or disclosure is required to lessen or prevent a serious threat to life, health or safety of a person or to public health and safety
- to locate a missing person
- where there is reason to suspect unlawful activity of a serious nature may be, or is being, engaged in relating to an agency's functions
- to establish, exercise or defend a legal or equitable claim
- for the purposes of a confidential alternative dispute resolution.

[Return to Table of Contents](#)

IDENTIFYING THE FUNCTIONS OR ACTIVITIES OF AN APP ENTITY

To determine whether a particular collection of personal information is permitted involves a two-step process:

1. identifying your agency's functions or activities
2. determining whether the collection of personal information is **reasonably necessary** for, or **directly related** to, one of those functions or activities.

[Return to Table of Contents](#)

DIRECTLY RELATED

A clear and direct connection must exist between the personal information being collected and an agency function or activity.

An agency's functions will be conferred either by legislation or an executive scheme or arrangement established by government. Identifying your agency's functions involves examining the legal instruments that confer or describe the agency's functions, including:

- Acts and subordinate legislative instruments
- the Administrative Arrangements Order made by the Governor-General
- government decisions or ministerial statements that announce a new government function.

Note: The activities of an agency will be related to its functions and include incidental and support activities, such as human resources, corporate administration, property management and public relations activities.

[Return to Table of Contents](#)

REASONABLY NECESSARY

The 'reasonably necessary' test is an objective test. It is whether a reasonable person who is properly informed would agree that the personal information being collected is reasonably required for one of the entity's functions or activities.

Factors to consider when determining whether a collection of personal information is reasonably necessary for a function or activity include:

- what is the primary purpose of collection?
- how will the information be used in undertaking the function or activity? For example, collection because the information may be needed for future activities would not be reasonably necessary.
- could you undertake the function or activity without that information, or by collecting a lesser amount of personal information?

We need to be able to explain how the 'reasonably necessary' test is met.

[Return to Table of Contents](#)

NOT REASONABLY NECESSARY

The Information Commissioner has previously ruled that collection of personal information was not reasonably necessary for an entity's function or activity in the following situations:

- a job applicant being asked if they had suffered a work-related injury or illness, when this was not relevant to the position being advertised
- a person applying to open a bank account being asked to complete an application form that included a question about marital status, when this had no bearing on the applicant's eligibility to open an account
- a medical practitioner photographing a patient for the patient's medical file, when this was not necessary to provide a health service.

[Return to Table of Contents](#)

OTHER EXAMPLES OF PERSONAL INFORMATION COLLECTION

Other examples of personal information collection that may not be reasonably necessary for an entity's functions or activities include:

- collecting all information on a person's drivers licence to establish if the person is aged 18 years or over
- collecting personal information about a group of people, when information is only required for some of those people.

[Return to Table of Contents](#)

APP 4 - COLLECTION OF UNSOLICITED PERSONAL INFORMATION

APP 4 imposes obligations in relation to receiving personal information which is not solicited by the entity.

Where an entity receives information it did not intend to collect, the entity must determine whether or not it could have collected the information under APP 3.

If we determine we **could not have** collected the information, we must destroy or de-identify the information as soon as practicable, but only if lawful and reasonable to do so and only if the information is **not** contained in a Commonwealth record. If the information can't be destroyed, APPs 5 to 13 apply.

If we determine we **could have** collected the information, then APPs 5 to 13 apply in relation to the information as if it had been solicited under APP 3.

Note: Unsolicited personal information which is kept by the receiving agency must be given the same privacy protection as solicited personal information.

[Return to Table of Contents](#)

APP 5 - NOTIFICATION OF THE COLLECTION OF PERSONAL INFORMATION

APP 5 requires that such steps (if any) as are reasonable in the circumstances must be taken to notify a person at, before, or as soon as practicable after, collection of their personal information. Specific matters we need to make people aware of under APP 5 requirements include:

- who the entity is and how to contact it
- any collection from a person other than the individual or without the individual's knowledge
- if collection of the information is required or authorised under Australian law
- the purpose for collecting the personal information
- the consequences if all or some of the information is not collected
- any other APP entity, body or person the information may be disclosed to
- information about the entity's privacy policy, including how the person can access their personal information and seek correction of that information, and the complaint handling process
- whether the entity is likely to disclose the information to overseas recipients and, if so, the countries in which these recipients are likely to be located.

[Return to Table of Contents](#)

PRIVACY NOTICES

A privacy notice is used to notify people when personal information is collected about them. Privacy notices must comply with APP 5.

The notice tells people what their information is being collected for, and how it may be used or disclosed.

A privacy notice should be included on all forms (including online), letters or products that collect personal information about a person.

[Return to Table of Contents](#)

GENERIC APP 5 PRIVACY NOTICE

Your personal information is protected by law, including the *Privacy Act 1988*, and is collected by (*Agency name*) for the assessment and administration of payments and services. This information is required to process your application or claim.

Your information may be used by the department or given to other parties for the purposes of research, investigation or where you have agreed or it is required or authorised by law.

You can get more information about the way in which (*Agency name*) will manage your personal information, including our privacy policy at (*Agency website*) or by requesting a copy from the department.

In some circumstances, it may be reasonable not to take any steps at all. For example, where an entity collects personal information from an individual on a recurring basis over a short period in relation to the same matter, and the individual is aware (or reasonably ought to be aware) that a separate notice will not be issued for each instance of collection.

If the form is collecting information about more than one person, it needs to be clear that the privacy notice applies to any person whose personal information is collected. This may mean more than one privacy notice needs to be included on the form, or references to the location of a privacy notice need to be made in different sections of the form.

[Return to Table of Contents](#)

SCENARIOS

SCENARIO QUESTION 1

Select the correct answer.

Marcus is a customer of the department. The department wants to collect information about the ethnic origin of its customers. This information will be used to provide targeted services to areas where there are high numbers of culturally and ethnically diverse customers.

What do we need to do when asking Marcus for this information?

- Seek consent from Marcus to collect this information, and provide Marcus with a privacy notice referring him to the department's privacy policy.
- Nothing, we can collect this information without consent, as it is related to our business.
- We cannot collect this information from Marcus, even if he consents.

Enter your answer(s):

[Return to Table of Contents](#)

SCENARIO QUESTION 2

Select the correct answer.

Ava has contacted the department to apply for a payment. She has sent in extra documents (that contain personal information) with her application even though the department does not need this information to process her application.

What do we need to do with this information?

- We are required to destroy it.
- We are not required to destroy or de-identify it.
- We are required to de-identify it.

Enter your answer(s):

[Return to Table of Contents](#)

SCENARIO QUESTION 3

Select the correct answer.

Tim's manager has asked him to draft a new form for collecting personal information from members of the public.

Does Tim need to include a privacy notice on the form?

- No, it is not necessary to advise members of the public about their privacy rights.
- No, the department's privacy policy is available on the internet, so there is no need to put a notice on the form.
- Yes, Tim should ensure a privacy notice which complies with APP 5 is included on the form.

Enter your answer(s):

[Return to Table of Contents](#)

KEY POINTS TO REMEMBER

APP 3 - COLLECTION OF SOLICITED PERSONAL INFORMATION

- We can only collect personal information if it is reasonably necessary for, or directly related to, our functions or activities.
- Higher standards are applied to the collection of sensitive information.
- Personal information can be collected from a third party if certain conditions are met.

[Return to Table of Contents](#)

APP 4 - COLLECTION OF UNSOLICITED PERSONAL INFORMATION

- If we determine we **could not have** collected the unsolicited personal information, we must destroy or de-identify the information if lawful and reasonable, and it is not contained in a Commonwealth record.
- If the unsolicited personal information is contained in a Commonwealth record, we are not required to destroy or de-identify the personal information, even if it is determined that we could not have collected the information under APP 3. We must handle the information the same way we handle solicited information.
- If we determine we **could have** collected the unsolicited personal information, then we must handle the information the same way we handle solicited information.

[Return to Table of Contents](#)

APP 5 - NOTIFICATION OF THE COLLECTION OF PERSONAL INFORMATION

- When we collect personal information, or as soon as practicable after we collect the information, we must notify the person of specific matters regarding who we are and how we deal with their information.

[Return to Table of Contents](#)

SUMMARY

Great! You should be able to:

- discuss the term 'consent'
- outline how to identify entity functions or activities

- discuss the term 'reasonably necessary'
- outline what a privacy notice is and why it is used
- summarise APP 3, APP 4 and APP 5
- identify work situations where APP 3, APP 4 and/or APP 5 will apply.

[Return to Table of Contents](#)

TOPIC 4 – DEALING WITH PERSONAL INFORMATION

Overview

This topic provides information on dealing with personal information.

Objectives

By the end of this topic, you should be able to:

- summarise APP 6, APP 7, APP 8 and APP 9
- identify work situations where APP 6, APP 7, APP 8 and/or APP 9 will apply.

[Return to Table of Contents](#)

APP 6 - USE OR DISCLOSURE OF PERSONAL INFORMATION

APP 6 outlines when we can use and/or disclose personal information for secondary purposes. Personal information can be used for the purpose for which it was collected (the primary purpose), but where it is to be used for a secondary purpose we will generally require the individual's consent unless the use or disclosure falls under one of these exceptions:

- the person would reasonably expect the use or disclosure for the secondary purpose, and the secondary purpose is **related** to the primary purpose (for personal information) or **directly related** to the primary purpose (for sensitive information)
- the use or disclosure is required or authorised by law
- the use or disclosure is reasonably necessary for the enforcement related activities conducted by, or on behalf of, an enforcement body (if an entity uses or discloses personal information for enforcement related activities, it must make a written note of the use or disclosure).
- the agency provides an enforcement body with biometric information or templates in accordance with guidelines made by the Commissioner
- a permitted general situation exists.

Some examples of permitted general situations are:

- where collection, use or disclosure is required to lessen or prevent a serious threat to life, health or safety of a person or to public health and safety
- to locate a missing person
- if there is reason to suspect unlawful activity of a serious nature may be, or is being, engaged in relating to an agency's functions
- to establish, exercise or defend a legal or equitable claim
- for the purposes of a confidential alternative dispute resolution.

[Return to Table of Contents](#)

APP 7 - DIRECT MARKETING

APP 7 regulates the use and disclosure of personal information by private sector organisations for the purpose of direct marketing.

Generally, private sector organisations may only use or disclose personal information for direct marketing purposes where the individual has either consented to their personal information being used for direct marketing, or has a reasonable expectation that their personal information will be used for this purpose, and conditions relating to opt-out mechanisms are met.

The provision relates to private sector organisations, not agencies. However, it is worth noting that APP 7 permits contracted service providers for Commonwealth contracts to use or disclose personal information for the purpose of direct marketing if:

- the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract, and
- the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

[Return to Table of Contents](#)

APP 8 - CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION

APP 8 necessitates an accountability approach to cross-border disclosure of personal information.

Before we disclose personal information to an overseas recipient, we must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to that information. In some circumstances an act done, or a practice engaged in, by the overseas recipient that would breach the APPs, is taken to be a breach of the APPs by the entity. There are only limited circumstances in which cross-border disclosure is permitted without taking reasonable steps to ensure that the overseas recipient does not breach the APPs (for example, where the disclosure is required or authorised under an international agreement).

This is of particular relevance when contemplating storage solutions used which may rely on technology solutions storing information overseas (cloud servers).

[Return to Table of Contents](#)

APP 9 - ADOPTION, USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS

APP 9 generally only applies to private sector organisations, prohibiting them from adopting, using or disclosing a government related identifier unless an exception applies. This can include use of drivers licence numbers, Medicare numbers and other similar identifiers for purposes of identification.

[Return to Table of Contents](#)

GOVERNMENT RELATED IDENTIFIER

An identifier of an individual that has been assigned by:

- an agency
- a State or Territory authority
- an agent of an agency, or a State or Territory authority, acting in its capacity as agent
- a contracted service provider for a Commonwealth contract, or a State contract, acting in its capacity as contracted service provider for that contract.

An 'identifier' is anything other than the person's name or ABN, and can include a number, letter or symbol that is used to identify a person or to verify the identity of a person.

[Return to Table of Contents](#)

ADOPTION OF GOVERNMENT RELATED IDENTIFIERS

A private sector organisation cannot adopt the government related identifier of a person as its own identifier, unless required or authorised by law.

[Return to Table of Contents](#)

USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS

A private sector organisation cannot use or disclose a government related identifier of a person unless the use or disclosure is required or authorised by law, a permitted general situation exists, or the use or disclosure is reasonably necessary:

- to verify the identity of the person
- to fulfil obligations to an agency or State or Territory authority
- for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Some examples of permitted general situations are:

- where collection, use or disclosure is required to lessen or prevent a serious threat to life, health or safety of a person or to public health and safety
- to locate a missing person
- if there is reason to suspect unlawful activity of a serious nature may be, or is being, engaged in relating to an agency's functions
- to establish, exercise or defend a legal or equitable claim
- for the purpose of a confidential alternative dispute resolution.

[Return to Table of Contents](#)

SCENARIOS

SCENARIO QUESTION 1

Select the correct answer.

Rajesh is a customer of the department who has been involved in a motor vehicle accident. He has suffered significant physical injuries and his insurer is taking legal action against the driver of the vehicle.

The department receives a request from Rajesh's insurer for copies of his personal information from the last six months.

Can the department disclose this information to the insurer?

- The department needs to get consent from Rajesh to disclose this information.
- The department can provide this information to the insurer without Rajesh's consent because it is a permitted general situation under the Privacy Act.
- The department cannot disclose this information to the insurer under any circumstances.

Enter your answer(s):

[Return to Table of Contents](#)

SCENARIO QUESTION 2

Select one or more as appropriate (please note there may be more than one correct answer).

Bob is a customer of the department. He is currently travelling and is in Vienna, Austria. Bob has access to the internet and logs on from Vienna. The information he accesses is routed through servers located in Istanbul.

Does APP 8 apply in this case?

Select all that apply, there may be more than one correct answer:

- No, Bob is accessing his own information. APP 8 only applies if Bob is not the person to whom the information relates.
- No, information being routed through an overseas server does not constitute a disclosure and so APP 8 does not apply.
- The department cannot provide access to online services from overseas locations in any circumstances.

Enter your answer(s):

[Return to Table of Contents](#)

KEY POINTS TO REMEMBER

APP 6 - USE OR DISCLOSURE OF PERSONAL INFORMATION

- Personal information can be used or disclosed for a secondary purpose (i.e. purpose different from the purpose it was collected for) in certain circumstances, including where the use or disclosure is authorised or required by law.
- We generally require the individual's consent where personal information is used or disclosed for a purpose unrelated to the reason it was collected (secondary purpose) unless an exception applies.

[Return to Table of Contents](#)

APP 7 - DIRECT MARKETING

- Private sector organisations may only use or disclose personal information for direct marketing purposes if the person consents, or has a reasonable expectation their personal information will be used for this purpose.

[Return to Table of Contents](#)

APP 8 - CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION

- Before disclosing personal information overseas, we need to take reasonable steps to ensure the overseas recipient does not breach the APPs, unless an exception applies.

[Return to Table of Contents](#)

APP 9 - GOVERNMENT RELATED IDENTIFIERS

- Private sector organisations are prohibited from adopting, using or disclosing a government related identifier, such as a drivers licence number or a Medicare number, unless an exception applies.

[Return to Table of Contents](#)

SUMMARY

Great! You should be able to:

- summarise APP 6, APP 7, APP 8 and APP 9
- identify work situations where APP 6, APP 7, APP 8 and/or APP 9 will apply.

[Return to Table of Contents](#)

TOPIC 5 - INTEGRITY OF PERSONAL INFORMATION

Overview

This topic provides information on the integrity of personal information.

Objectives

By the end of this topic, you should be able to:

- summarise APP 10 and APP 11
- identify work situations where APP 10 and/or APP 11 will apply.

[Return to Table of Contents](#)

APP 10 - QUALITY OF PERSONAL INFORMATION

APP 10 requires an entity to take reasonable steps to ensure the personal information it collects is accurate, up to date and complete.

We must also ensure the personal information we use or disclose is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

[Return to Table of Contents](#)

APP 11 - SECURITY OF PERSONAL INFORMATION

APP 11 requires an entity to take reasonable steps to ensure personal information it holds is protected from misuse, interference, loss, unauthorised access, modification or disclosure.

The inclusion of 'interference' recognises that attacks on personal information may not be limited to misuse or loss and may include interference that does not amount to modification of the information.

Preventing interference may require additional measures to be taken to protect against computer attacks and other interferences of this nature.

[Return to Table of Contents](#)

APP 11 imposes a requirement on entities to take reasonable steps to destroy or de-identify personal information we no longer need for any authorised purpose, unless:

- it is contained in a Commonwealth record (noting that this will cover most personal information held by agencies)
- we are required by or under an Australian law or a court/tribunal order to retain the information.

[Return to Table of Contents](#)

SCENARIO

SCENARIO QUESTION 1

Select the correct answer.

The hacker group, Anonymous, has hacked into the department's IT system and published the personal information of all its customers. During the course of an internal investigation, it is discovered that the security software the department has been using is out of date and has not been updated for seven years.

Is the department in breach of APP 11?

- No, because the department has security software in place it has met the obligations of APP 11 and no APP breach has occurred.
- Yes, the department must take reasonable steps to protect information, and as the security software is significantly out of date the Information Commissioner may find a breach of APP 11 has occurred.
- No, APP 11 does not apply to cyber-attacks.

Enter your answer(s):

[Return to Table of Contents](#)

KEY POINTS TO REMEMBER

APP 10 - QUALITY OF PERSONAL INFORMATION

- We must ensure the personal information we collect, use or disclose is accurate, up to date, complete and relevant.

[Return to Table of Contents](#)

APP 11 - SECURITY OF PERSONAL INFORMATION

- We are required to ensure the personal information we hold is protected from misuse, interference, loss, unauthorised access, modification or disclosure.

[Return to Table of Contents](#)

SUMMARY

Great! You should be able to:

- summarise APP 10 and APP 11
- identify work situations where APP 10 and/or APP 11 will apply.

[Return to Table of Contents](#)

TOPIC 6 – ACCESS TO, AND CORRECTION OF, PERSONAL INFORMATION

LEARNING OBJECTIVES

Overview

This topic provides information on the access and correction of personal information.

Objectives

At the end of this topic, you should be able to:

- summarise APP 12 and APP 13
- identify work situations where APP 12 and/or APP 13 will apply.

[Return to Table of Contents](#)

APP 12 - ACCESS TO PERSONAL INFORMATION

APP 12 requires an entity to give a person access to the personal information it holds about that person, unless refusal is required or authorised under the *Freedom of Information Act 1982* (FOI Act) or any other Commonwealth or Norfolk Island law that provides for access to documents.

APP 12 imposes a requirement for agencies to respond to requests for access within 30 days. We must give access in the manner requested by the person if it is reasonable and practicable to do so. We must not charge the person for making the request or giving access to the personal information.

If an entity refuses to give access, or to give access in the manner requested, we must take reasonable steps to give access to the personal information in an alternative way, for example, using a mutually agreed intermediary.

If an entity refuses to give access to the personal information we must give the person a written notice with the reasons for refusal and include information on how the person may complain about the refusal.

The APPs do not provide for an extension to the 30-day timeframe to respond to requests for access to personal information.

[Return to Table of Contents](#)

APP 13 - CORRECTION OF PERSONAL INFORMATION

APP 13 requires an entity to take reasonable steps to correct personal information to ensure it is accurate, up to date, complete, relevant and not misleading at the request of the person, or where the entity is satisfied the information needs to be corrected.

This applies when individuals request correction and where the need for correction is identified by a third party or the department.

Similar to APP 12, correction requests by the individual must be responded to within 30 days, must not be charged for, and when refusing a person's correction request we must provide the person with written reasons for the refusal and notify them of available complaint procedures.

APP 13 imposes obligations where personal information has been corrected and that personal information has been previously disclosed to another APP entity. We must take reasonable steps to notify that other entity of the correction if requested by the person, unless it is impracticable or unlawful to do so.

If an entity refuses to correct personal information, the person can request a statement stating the information is inaccurate, out of date, incomplete, irrelevant, or misleading. The statement must be attached to the information so it is clear to users of the information.

[Return to Table of Contents](#)

SCENARIOS

SCENARIO QUESTION 1

Select one or more as appropriate (please note there may be more than one correct answer).

Zara is a customer of the department. One day she receives a letter from the department and notices her name is misspelled. She contacts the department the next day and asks for a copy of her record to check the spelling of her name.

What are our obligations to Zara?

- To provide Zara with her record within 30 days of her making the request.
- Zara has the right to ask us to correct the spelling of her name and we are required to do this within 30 days of her making the request.
- We have no obligation under the Privacy Act to provide Zara with this information. She should make her request under the *Freedom of Information Act 1982*.
- We are not required to amend Zara's record to reflect the correct spelling of her name.
- Zara needs to put her request in writing before we will consider providing her with access to her record or amending her record.

Enter your answer(s):

[Return to Table of Contents](#)

SCENARIO QUESTION 2

Select one or more as appropriate (please note there may be more than one correct answer).

Alex is a departmental staff member. One day he is assisting Mike, a customer, and notices that some of the information on Mike's record does not belong to him.

Alex investigates further and finds the information belongs to another customer with the same name as Mike. Alex also notices the incorrect information has been provided to another department.

What are we required to do?

- Amend Mike's record to remove the incorrect information as soon as practicable.
- Take action to amend Mike's record to remove the incorrect information within 30 days.
- Contact the other department to advise them of the error, if Mike asks us to do so.
- We do not have to do anything as Mike is not aware of the error.

Enter your answer(s):

[Return to Table of Contents](#)

KEY POINTS TO REMEMBER

APP 12 - ACCESS TO PERSONAL INFORMATION

- We must give a person access to their own personal information unless a specific exception applies.

- We must respond to requests for access to personal information within 30 days, free of charge, and provide written reasons if refusing the request for access.

[Return to Table of Contents](#)

APP 13 - CORRECTION OF PERSONAL INFORMATION

- We must take certain steps to correct personal information where that information is inaccurate, out of date, incomplete, irrelevant or misleading.
- We must respond to requests from an individual for correction of their personal information within 30 days, free of charge, and provide written reasons if refusing the correction request.

[Return to Table of Contents](#)

SUMMARY

Great! You should be able to:

- summarise APP 12 and APP 13
- identify work situations where APP 12 and/or APP 13 will apply.

[Return to Table of Contents](#)

TOPIC 7 – CODE REQUIREMENTS

LEARNING OBJECTIVES

Overview

This topic provides information regarding requirements under the *Australian Government Agencies Privacy Code* ('the Code') which affect all government agencies.

Objectives

At the end of this topic, you should be able to:

- summarise requirements under the Code
- know what a Privacy Impact Assessment is, and when to do one
- know where to go to obtain further information regarding privacy.

[Return to Table of Contents](#)

AUSTRALIAN GOVERNMENT AGENCIES PRIVACY CODE

The *Privacy (Australian Government Agencies – Governance) APP Code 2017* ('the Code') took effect from 1 July 2018 and imposes mandatory requirements for the handling of personal information by government agencies.

The aim of the Code is to promote a 'privacy by design' approach to ensure that privacy compliance is included in the design of information systems and practices from their inception. It does this by requiring agencies to take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs and any binding registered APP code.

What's required under the Code?

The following key requirements for agencies to adopt under the Code are to:

- have a **privacy management plan**

This is a plan which outlines how the agency will meet its APP compliance obligations.

- have a designated **Privacy Officer**
The Privacy Officer is the primary point of contact for advice on privacy matters in the agency, and must perform a number of functions under the Code.
- have a designated **Privacy Champion** (who is a senior official within the agency)
The Privacy Champion must promote a culture of privacy within the agency that values and protects personal information, as well as performing a number of other functions.
- undertake **privacy impact assessments** (PIAs) for all 'high privacy risk' projects, maintain a register for those PIAs, and publish the register
This is an assessment of the privacy impacts of a project or changed way of handling personal information. Further information regarding PIAs is below.
- provide appropriate **privacy education or training** to agency staff at induction and annually thereafter for staff with access to personal information.

PRIVACY IMPACT ASSESSMENTS (PIA)

The Code directs that all agencies must conduct a PIA for all **high privacy risk** projects, and states that a project may be high privacy risk if:

The agency reasonably considers that the project involves any new or changed ways of **handling personal information** that are likely to have a significant impact on the privacy of individuals.

'**Handling personal information**' means dealing with personal information in any way, including managing, collecting, holding, using or disclosing personal information.

The first step to determine whether a PIA is required under the Code is to conduct a 'threshold assessment'. This involves answering the following three questions:

1. Will any personal information be collected, stored, used or disclosed in the project?
2. Does the project involve any new or changed ways of handling personal information?
3. Is the project likely to have a **significant impact** on the privacy of individuals?

A '**significant impact**' can be assessed by taking into account:

- the number of individuals whose personal information will be handled (is it 50 or 5000?)
- the type of personal information involved, and whether it includes sensitive information such as a person's racial or ethnic origin, criminal record or health information
- the number of third parties who will have access to the personal information.

If the answer to all three questions is 'yes', a PIA will be required under the Code. If a threshold assessment decision is made not to proceed with a PIA, a written copy of the threshold assessment should be retained.

'**Privacy impact assessment**' is defined in the Privacy Act (s 33D) as:

a written assessment of an activity or function that:

- a) identifies the impact that the activity or function might have on the privacy of individuals; and
- b) sets out recommendations for managing, minimising or eliminating that impact.

Video: <https://www.oaic.gov.au/elearning/pia/topic1.html>

The Office of the Australian Information Commissioner (OAIC) has further information regarding how to conduct a PIA. If you require additional information or assistance, please visit the OAIC website or contact your agency's Privacy Officer.

Your agency is required to maintain a register of PIAs it conducts, and must publish the register, or a version of the register, on its website. The Privacy Officer has responsibility to ensure the agency complies with this obligation.

TOPIC 7 - KNOWLEDGE CHECK

To test your knowledge of the information presented in this topic, answer the following questions.

QUESTION 1

Select one or more as appropriate (please note there may be more than one correct answer).

Dave's agency is considering changing IT infrastructure and engaging with other agencies to better share information to improve service delivery and assurance activities, which will impact the way in which customers' personal information is used and stored.

What does Dave need to do?

- There may be some privacy implications so Dave should report these to the Office of the Australian Information Commissioner.
- It is likely the project involves new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals, therefore Dave needs to conduct a privacy impact assessment.
- Nothing. The agency got people's permission at the time their personal information was collected, so it can do anything with that information.

Enter your answer(s):

QUESTION 2

Select one or more as appropriate (please note there may be more than one correct answer).

Alison works in a compliance role within her department and, as such, has access to complete client records to allow her to actively monitor service delivery and compliance.

How often should Alison complete privacy training?

- Alison should have completed privacy training as part of her induction.
- As someone who has access to personal information, Alison should refresh her privacy training every 6 months.
- As someone who has access to personal information, Alison should refresh her privacy training annually.
- Alison doesn't need to complete any privacy training.

Enter your answer(s):

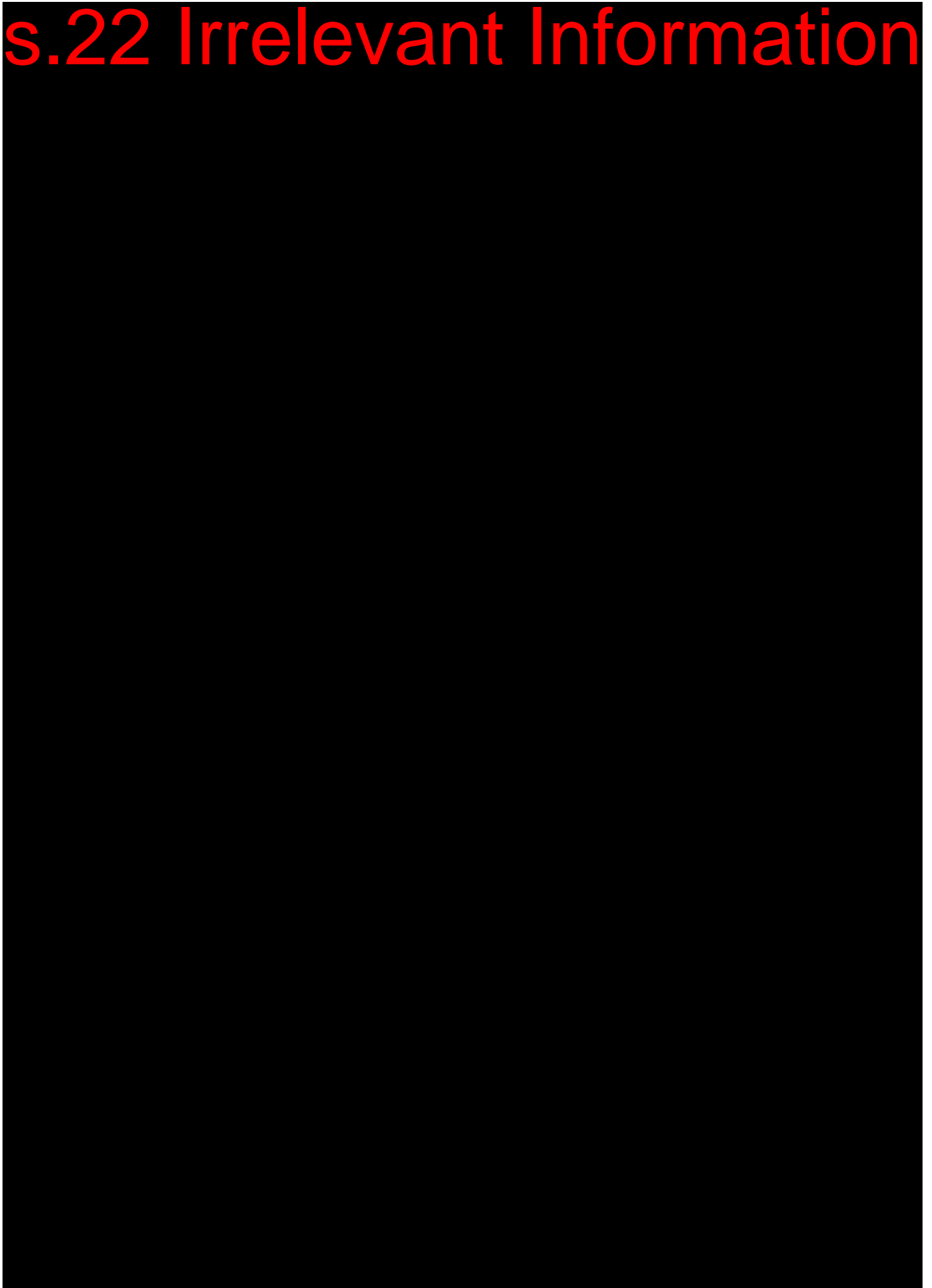
KEY POINTS TO REMEMBER

AUSTRALIAN GOVERNMENT AGENCIES PRIVACY CODE

- The Code promotes a 'privacy by design' approach to ensure that privacy compliance is included in the design of information systems and practices from their inception.
- Every agency must have a Privacy Officer and Privacy Champion, who have specific functions under the Code.
- Privacy impact assessments (PIAs) must be completed for all high privacy risk projects.
- All staff should complete appropriate privacy training at induction and annually thereafter for those with access to personal information.

[Return to Table of Contents](#)

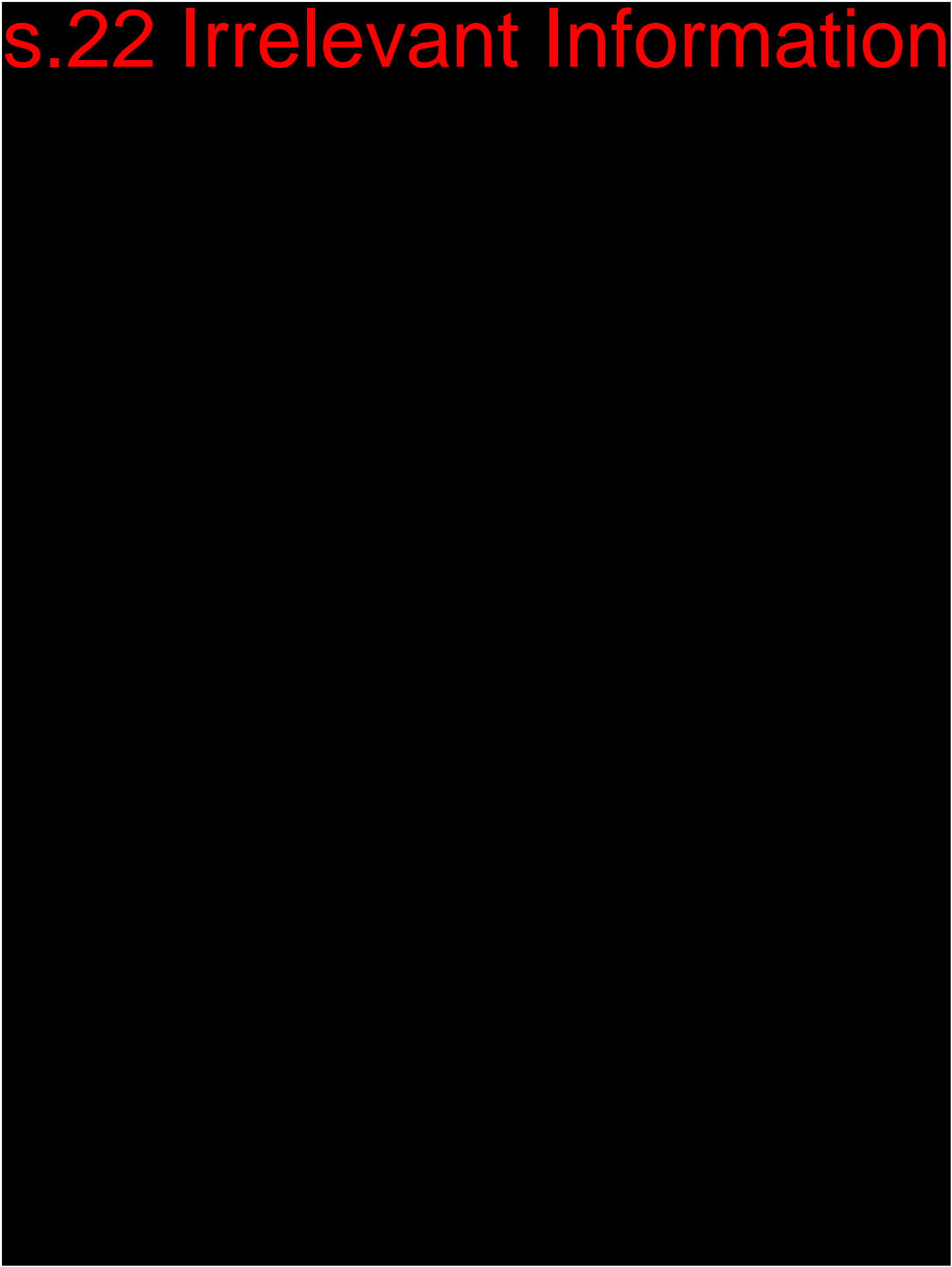
s.22 Irrelevant Information



s.22 Irrelevant Information



s.22 Irrelevant Information



Privacy



The purpose of this module is to provide you with a refresher of the Office of the Fair Work Ombudsman (OFWO) **privacy protocols**.

☰ Introduction

☰ Overview

☰ The Australian Privacy Principles

☰ Identifying personal information

☰ Applying the Privacy Principles in your role

☰ Privacy breaches

☰ Privacy knowledge check

☰ Conclusion

Lesson 1 of 8

Introduction



The journey towards reconciliation, Jordan Lovegrove

The Fair Work Ombudsman acknowledges the Traditional Custodians of Country throughout Australia and their continuing connection to land, waters and community.

We pay our respect to them and their cultures, and Elders, past, present and future.

The purpose of this module is to provide you with a refresher of the Office of the Fair Work Ombudsman (OFWO) **privacy protocols**.



“Learning outcomes

After completing this module, you will be able to:

- identify information defined as personal
- explain how privacy affects your work.



“Duration

You should allow **15 minutes** to complete this module.”

CONTINUE

Documents released by the Fair Work Ombudsman
Under the Freedom of Information

Overview



"CONSIDER

Would it make you feel uncomfortable if people you do not know could find your contact details or knew where you live?

Imagine if your health records were something people could look up at their leisure?

I bet it fills you with dread! And so it should."



Private sign

Luckily, we all have the legal right to have our personal information protected.

The Privacy Act 1988 (Privacy Act) protects your privacy by setting rules for how government and some businesses collect and handle your personal information.



"CONSIDER

Now, let's think about the role of the Office of the Fair Work Ombudsman (OFWO). We collect and investigate a broad range of personal information to provide our service to the Australian public.

We must follow the requirements set out in the Privacy Act to safeguard personal information."

We also need to look after the personal information we keep for OFWO staff.

We collect your information for activities such as:

- your police check from when you started out here in the OFWO
- documents you provide to access your leave entitlements.

This learning provides you with the information you need to know to help keep the personal information of the Australian public (including yours and your coworkers) protected.

CONTINUE

The Australian Privacy Principles

The Privacy Act provides us with the Australian Privacy principles (APP), described as 'the cornerstone of the privacy protection framework in the Privacy Act'. The APPs provide us with clear privacy guidelines in plain English terms.



"MORE INFORMATION

You should review the APPs on the Office of the Australian Information Commissioner (OAIC) website if you want to find out more information about each principle.

The easiest way to get to the APPs is to search '**Australian Privacy Principles**' in your browser."

The following are summaries of key APPs that apply most to the work we do.

Open and transparent management of personal information —

One of the ways we achieve this by publishing and maintaining our privacy policy on our website.

If a member of the public needs to read our Privacy Policy, you can guide them to it by asking them to go to our [fairwork.gov.au](https://www.fairwork.gov.au) website and searching 'privacy'.

Give someone the option to remain anonymous or use a pseudonym —

We must apply this option where it is practical for us to do so.

For example, we allow individuals the choice to make an anonymous report on our website.

Collection of solicited personal information —

Requires that we only collect personal information that is necessary for us to complete our work. If we need to collect sensitive information, we must get the individual's consent first in most circumstances.

Dealing with unsolicited personal information —

There may be circumstances where we receive unsolicited personal information that we didn't request.

The APP requires that we destroy or de-identify that information in line with government archiving requirements as soon as practical.

Please follow the OFWO's processes on the 'Disposal of information' Intranet page before you destroy information.

Notification of the collection of personal information —

When we collect personal information, we provide collection statements that describe how we handle it.

For example, when we contact someone for evidence as part of an investigation and they provide their own personal information.

We must notify or make an individual aware of all personal information that we collect about them, whether we collect it directly or from a third party.

An example is how we describe a person's online privacy rights while using our website. We do this on our website's Privacy page.

Use or disclosure of personal information —

We can only use or disclose personal information for the primary purpose for which we collected it.

There are limited exemptions to this rule, such as where an individual has given us their consent for secondary use, or it is required to help enforcement bodies with their activities.

Quality of personal information —

We must maintain the personal information we use so that it is accurate, up-to-date and complete for the purpose we are using it for.

Security of personal information —

We must take reasonable steps to protect the personal information we hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.

We can take personal responsibility for this by keeping personal information in the systems designed to keep it protected.

Access to personal information —

This Principle requires that we must give an individual access to their own personal information if they ask us (in most circumstances).

It applies alongside the Freedom of Information Act 1982 which provides a right to request access to all government information.

Correction of personal information —

We must correct any incorrect personal information we use.

We can do this when we identify the personal information is incorrect, or when the individual requests we correct it.

CONTINUE

Identifying personal information



"CONSIDER

We collect various personal and sensitive personal information here at the OFWO.

Do you know how to identify personal information and sensitive personal information from other information?"

Below are definitions to help you:

Personal information

Personal information is information or an opinion, whether recorded in a material form or not, whether true or not, about an identified individual or an individual who is reasonably identifiable.

Sensitive personal information

Sensitive personal information is information that may have traditionally led to discrimination against the individual. The formal definition in the Privacy Act is a list of specific types of information.



"CONSIDER

Take a moment to think about the personal information you access or use in your role. How many different types can you think of?"

Select all the descriptions of information below describing

Personal information which are not sensitive.

Business name

Comments recorded about a person's sexual orientation

Date of birth

- An OFWO employee's signature
- A description of a person's religious belief
- Photos of the inside of a workplace (without employees)
- A person's address
- A person's health information
- A photo of an individual's car

SUBMIT

CONTINUE

Applying the Privacy Principles in your role

After learning about the APPs and honing your skills in identifying personal information, you may have already developed a better understanding of how you can help us meet our privacy requirements.

The following are 5 examples of role specific behaviours that we must develop to maintain our privacy requirements.

Keep personal information secure

You have probably heard these requirements many times. There is a reason for it! The following behaviours are foundational to maintaining privacy:

- Keep personal information in the systems or secure containers designed to store it in.
- Maintain a clear desk and screen.
- Identify sensitive and security classified information by using applicable protective markings.
- Restrict access to personal information to a need-to-know basis.

Know what information we shouldn't collect

Our Privacy Policy is available from our Intranet and is available to the public through our website. It tells us that we should not collect the following:

- Tax File Numbers, in most circumstances.
- Covert recordings.
- Health information.

If we receive this as unsolicited information, we must take steps to either de identify it or destroy it. If you are unsure, please contact your friendly Privacy Officer for advice.

Notify people when we collect their personal information

We need to explain the following when we collect personal information directly or from a third party:

- who we are where it is not clear we work for the OFWO
- whether we are required to collect it by law
- why we are collecting it
- who we share it with.

We can do this verbally or in writing.

Check, double check and triple check – just to make sure!

Many of the privacy breaches we investigate are due to human error. If you are sharing information, you must take the appropriate steps to makes sure you are only sharing with the people that you need-to-share with, for example:

- If you are sending an email that contains personal information, make sure you check the recipients before you send.
- If you are sharing personal information using Microsoft 365 tools, make sure you check the share settings. The default settings are not always appropriate.

Know how to access our Privacy Policy —

You can access our Privacy Policy simply by searching 'privacy' on our Intranet.

Our Privacy Intranet page summarises our privacy requirements here in the OFWO and contains links to our policy documents and external links web pages like the Australian Privacy Principles.



Our customers can find our Privacy Policy on our fairwork.gov.au website. If you need to guide them, it is as simple as asking them to search 'Privacy' from our website's search function.

Our Privacy Policy explains the types of personal information we collect and the sources we collect it from. It explains how we use it, store it and for how long we need to keep it.

Please practice accessing our privacy information through the Intranet and our website. This will increase your confidence when you need to access it next.

Watch the video below to find out how you can protect personal information when using email (3:35)

View video transcript:

	How you can protect personal information when using email - video transcript.pdf 139.1 KB	
---	---	---

TASK

Search for the **Privacy Policy** on the Intranet

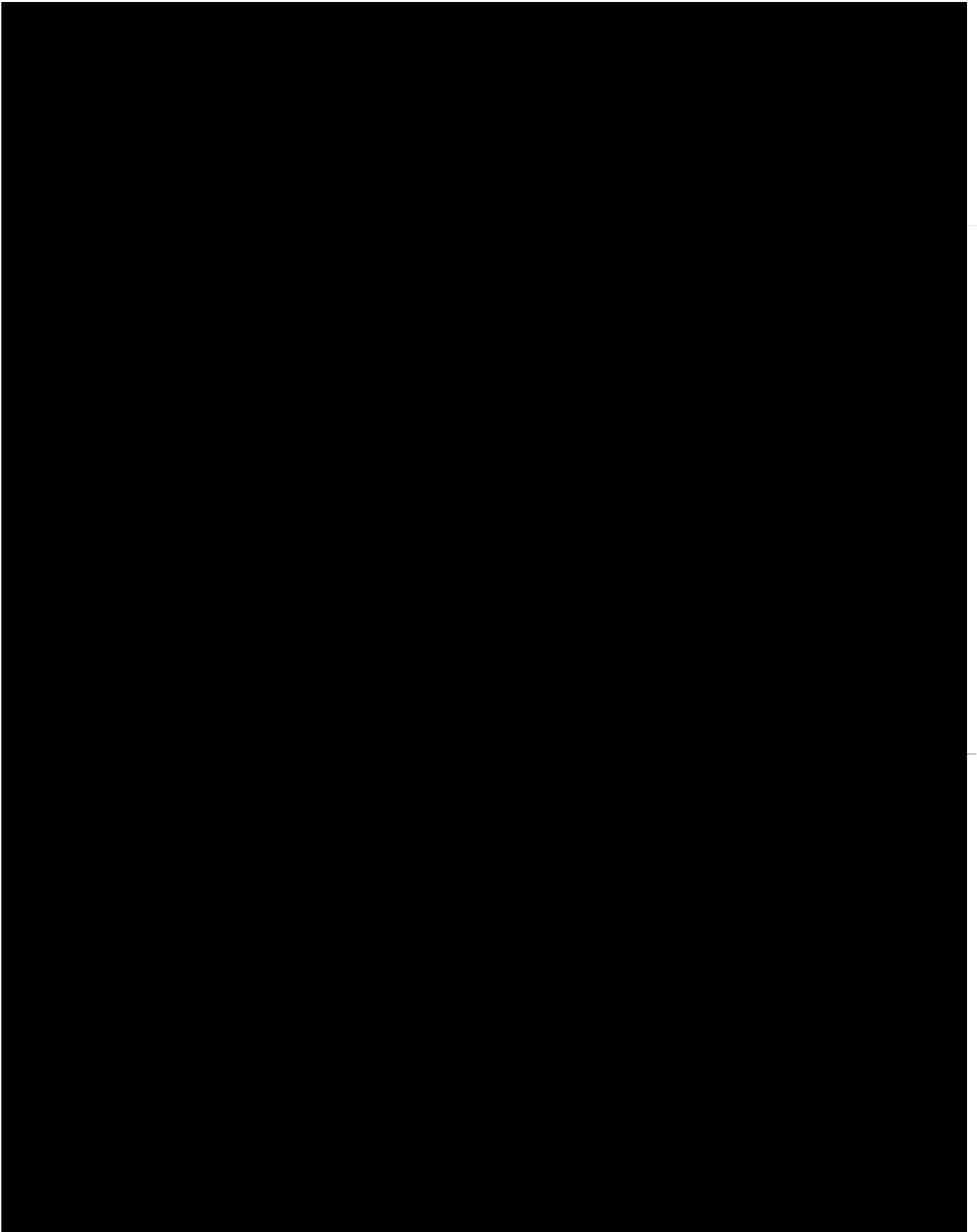
INTRANET

Search for the **Privacy Policy** on the FWO website

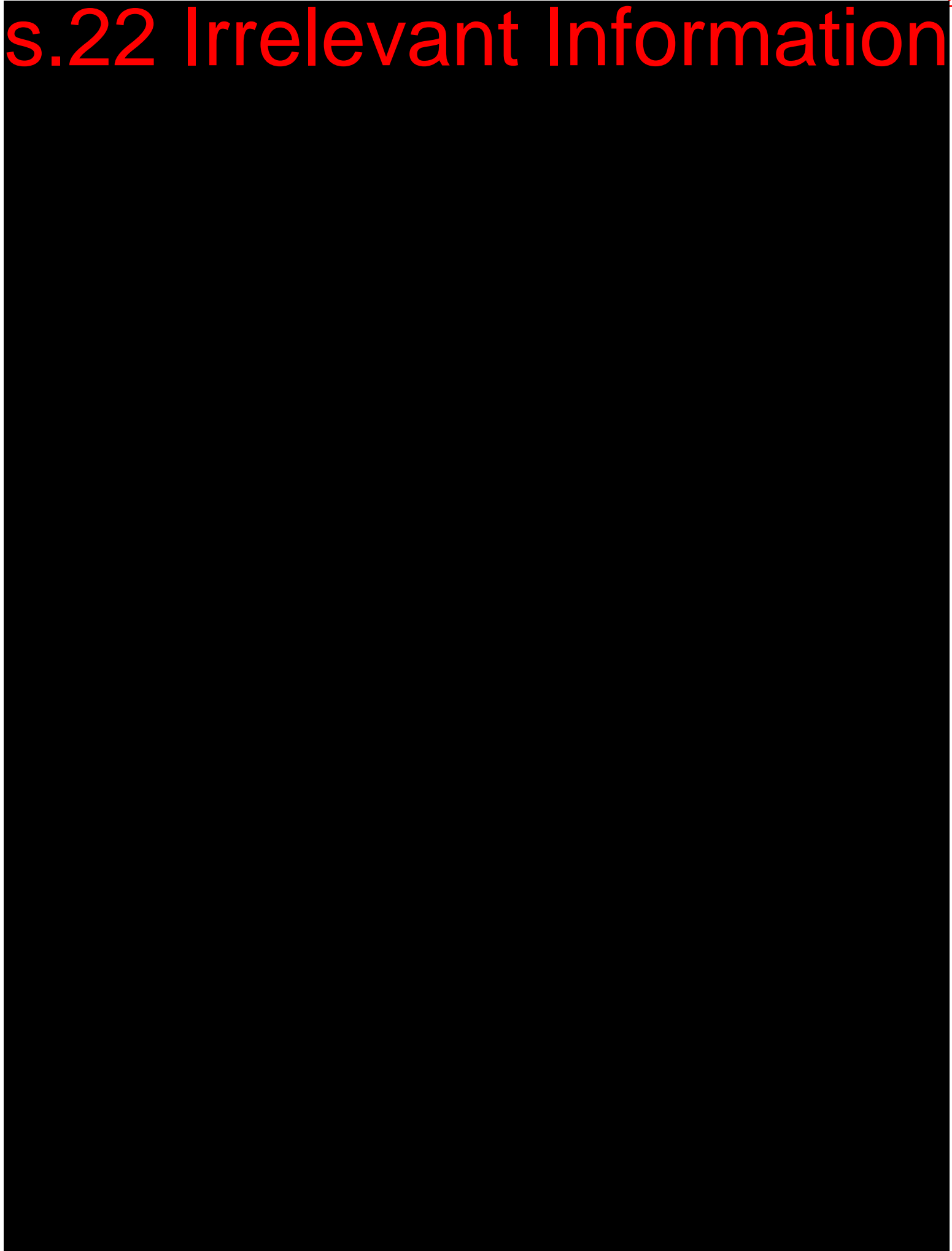
FWO WEBSITE

CONTINUE

Documents released by the Fair Work Ombudsman
Under the Freedom of Information



s.22 Irrelevant Information



Lesson 7 of 8

Privacy knowledge check

Privacy is...

(Select all that apply)

- a human right
- making sure the government doesn't share information
- the right to be left alone
- controlling your identity
- having something to hide
- using a password manager

SUBMIT

Based on what you have learnt, select the sensitive personal information from the following:

(Select all that apply)

-
- Age
 - Sexual orientation
 - Religious beliefs
 - Political opinions
 - A person's address

SUBMIT

Select the correct ways to use personal information from the following:

(Select all that apply)

- Allow individuals using our website to stay anonymous.
- Email case information to your personal email so you can work on it at home from your personal computer.
- Collect sensitive personal information from all employees when conducting a workplace inspection.
- Provide images of people and their formal documents to the Australian Federal Police in a suspected Human Trafficking case.
- Access internal WHS systems to find out why your coworker is limping.

SUBMIT

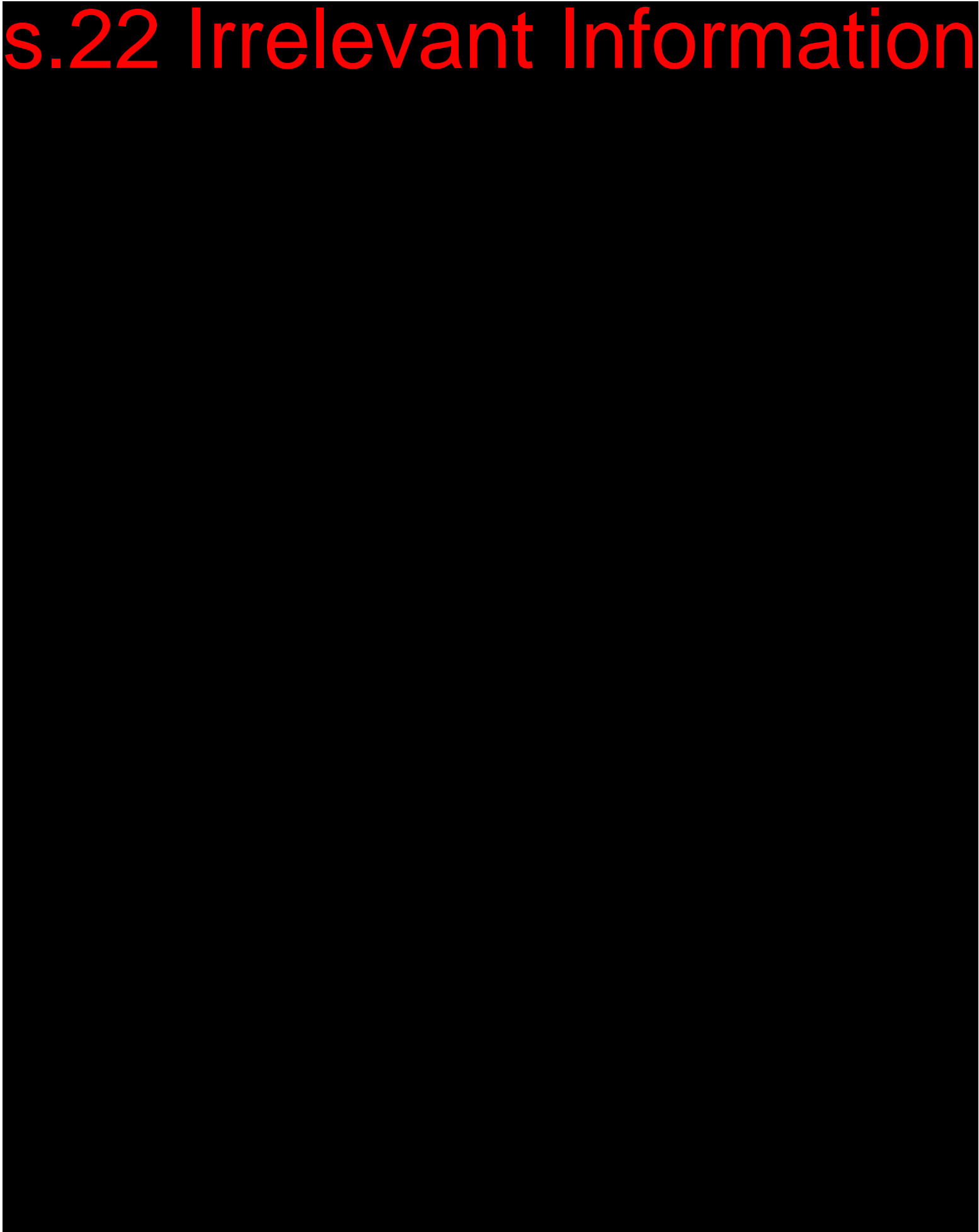
Which of the following behaviours are essential for you to develop to keep personal information secure?

(select all that apply)

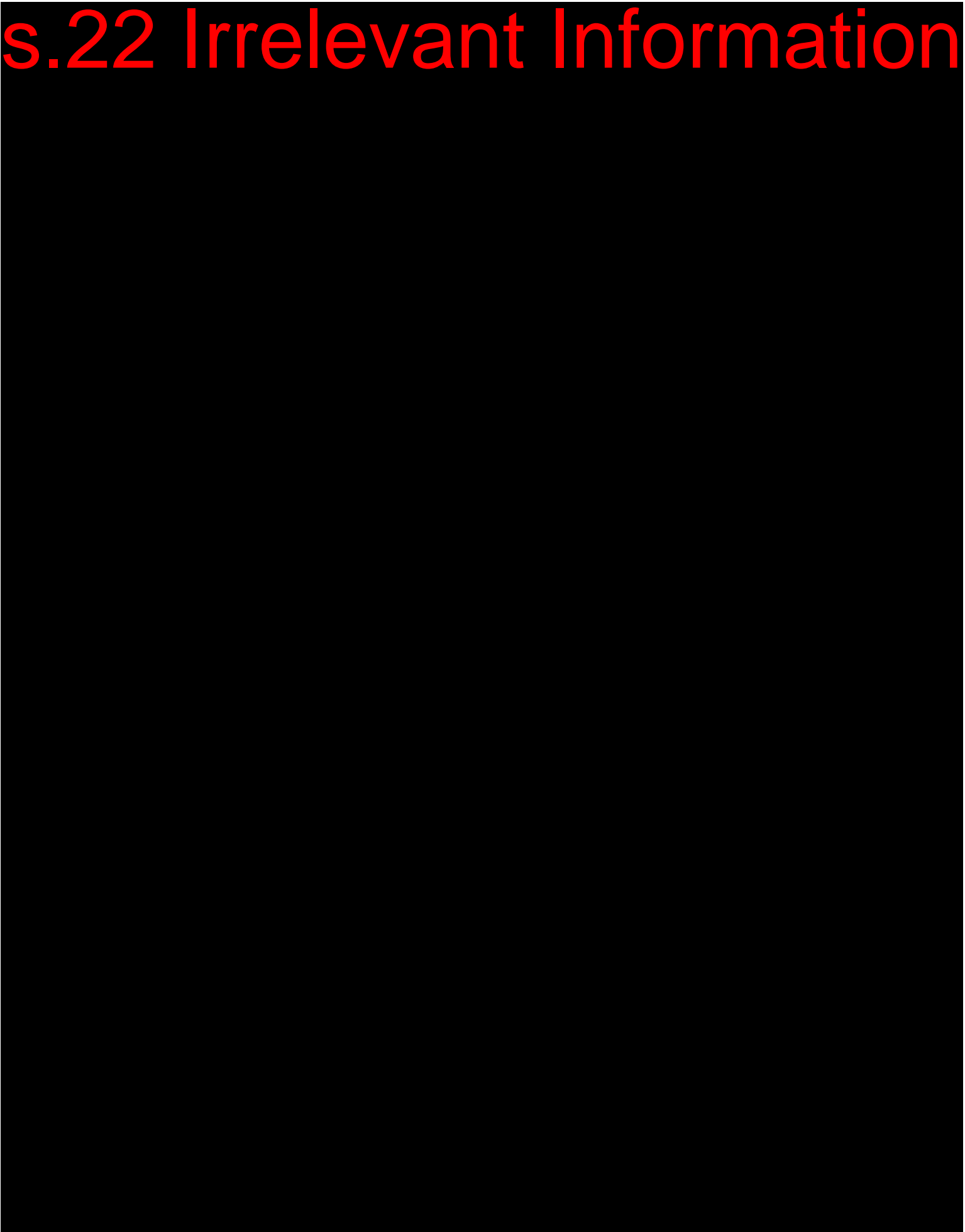
- Restrict access to personal information to a need-to-know basis.
- Maintain a clear desk and screen.
- Share it with your manager only
- Use applicable protective markings
- Save it in a shared Docbank folder that only your team can access.
- Keep it in specially designed systems or secure containers

SUBMIT

s.22 Irrelevant Information



s.22 Irrelevant Information



Lesson 8 of 8

Conclusion

Well done! You have successfully completed the **Privacy** refresher course.

You can come back at any time to review the content.



"You should now know:

- how to identify information defined as personal
- how privacy affects your work.

Select the **Exit** button to return to the Privacy refresher course page:

EXIT

Documents released by the Fair Work Ombudsman
Under the Freedom of Information