Information Commissioner
NORTHERN TERRITORY

Annual Report

2022/23

Access to Information | Privacy Protection

Acknowledgement of country

We pay respect to the past, present and future Traditional Custodians and Elders of lands throughout the Northern Territory.

Table of Contents

Message from the Commissioner

FOI numbers still on the rise

The annual total of Freedom of Information (**FOI**) access applications made to NT public sector organisations (**Organisations**) under the *Information Act 2002* (the **Act**) continues to grow. This year, there were 1,670 FOI applications received by Organisations — an increase of 3% compared with 2021/22 and over double that received six years ago. Notably, Territory Families, Housing and Communities has experienced an 80% increase in applications received in the last two years, rising from 245 in 2020/21 to 441 in 2022/23, due in part to people seeking information for the Stolen Generations Redress Scheme and the National Redress Scheme (Child Sexual Abuse).

In contrast to the increase in FOI applications to Organisations, the number of complaints to our Office has fallen markedly from a record high in 2020/21 of 42 to 15 this reporting period (equivalent to numbers received 5 years ago). Although encouraging, quite why increased numbers of FOI applications are not currently translating to more complaints is hard to discern. It may be that Organisations, many of whom are now supported by a centralised FOI Unit, are providing better service to applicants at first instance, providing fewer causes for complaint. In a smaller jurisdiction with fewer numbers, it takes time to divine the reasons for trends which can be easily affected by random factors. We will continue to monitor future developments with interest.

Privacy (Data) Protection

Data privacy is an area of growing importance to Organisations, particularly noting the amount of personal information stored electronically, the seemingly growing potential for privacy (data) breaches to occur and the damage they can do to individuals and to an Organisation's reputation. Historically, the only information we had on data privacy concerns was based on the small number of complaints received by our Office and queries raised by Organisations about how to handle a particular breach.

More recently, we have been asking for more information from Organisations about privacy complaints dealt with by them during each reporting period. This year, Organisations reported they dealt with 66 privacy complaints (55 from this reporting period and 11 carried over from the previous). Feedback from some agencies however, suggests that these numbers are likely to be an under-reporting of privacy complaints received. In many Organisations, complaints about privacy breaches are not dealt with by a centralised unit but within individual work units, and numbers may not be well reported. Most of these complaints appear to have been adequately addressed by the Organisations, as only seven privacy complaints were received by our Office during the period.

Organisations separately advised us of eight data (privacy) breaches that occurred during this reporting period. Noting that there is no requirement for Organisations to advise us of data breaches, the small number we become aware of may be a significant under-representation of the true numbers.

From my experience, I can confidently state that more needs to be done by Organisations and across the public sector to ensure that staff training, policies and processes are in place so that the public can trust that the personal and sensitive information held about them is safe and secure and used only for proper purposes. It is pleasing that some Organisations are taking steps to improve their performance in this regard but more work is necessary.

One initiative that deserves strong consideration is the introduction of a statutory mandatory data breach notification scheme to require notification to affected people and to my Office of serious data (privacy) breaches. The Commonwealth and NSW have already implemented statutory notification schemes to ensure that data breaches are properly reported. It is time for the NT to follow suit.

Privacy impact assessments

The growing prominence of privacy concerns and the relative ease with which mistakes can be made in a technology-rich environment (where one errant press of a button can disclose a warehouse worth of personal information) means any project that stores or uses personal information must appreciate and plan for the heavy risks involved.

Planning for privacy protection must be built into project planning. This is true not only for ultimate operational systems but equally for development stages where personal information may be inadvertently or necessarily collected, stored, used or disclosed.

An essential part of this planning is the conduct of privacy impact assessments. There is a tendency by some to shy away at the prospect of first, having to spend limited resources on such planning and second, having to commit further resources to address the issues it might raise.

However, the earlier that privacy considerations are brought into the mix, the easier it will be to effectively address privacy issues as part of the core solution. Avoiding proper planning merely lays the groundwork for fundamental errors and costly privacy fixes when major problems emerge at a later date that incur reputational damage and even greater commitment of resources to cobble together a Band-Aid solution.

Information sharing

During the year, we provided considerable advice to Organisations involved in the development of data access agreements and a technological solution to fully inform Territory Families when making decisions about vulnerable children. As I noted in last year's report, this is a very broad information sharing scheme involving details about a substantial number of Territory families, held by bodies as diverse as NT Police, Health, Education, Courts and Correctional Services. The privacy considerations are significant and our Office has continued to work with Organisations to ensure that the right balance is maintained to prioritise child protection with due regard maintained for privacy protection. That project is ongoing.

Work has also continued on the statutory review of an information sharing scheme under Part 5A of the *Domestic and Family Violence Act 2007*. The Review Report is in its final stages and should be provided to the relevant Minister in the near future.

Information Act review

The anticipated review of the Act has not progressed significantly during this reporting period, although some work has been done by NTG organisations to identify the relevant issues that require consideration in the areas of FOI, privacy and records management. There is no current publicised timeframe for this work to be progressed further but we remain an interested stakeholder in the process.

Acknowledgement of staff

As with any small independent office, the most important resource we have is our staff members. I recognise their contribution, including particularly that of the Deputy Commissioner, and commend them on their professionalism and commitment throughout the reporting period.

Peter Shoyer
Information Commissioner
28 September 2023

Introduction

The *Information Act 2002* (the **Act**) is the legislation governing freedom of information (**FOI**), privacy protection, and public sector records management in the NT. The Act provides for reasonable public access to government information, the responsible collection, correction and handling of personal information and appropriate records and archives management.

The Act is intended to strike a balance between competing interests of openness and transparency and the legitimate protection of some government information, including personal information about individuals.

The Act establishes an Information Commissioner to oversight information access and privacy protection provisions. The Information Commissioner's functions include:

- dealing with complaints about FOI decisions and privacy issues through an investigation and mediation process;
- referring, at the request of a party, dismissed or unresolved complaints to the NT Civil and Administrative Tribunal (**NTCAT**) for hearing;
- commenting on the privacy implications of new legislation and new government initiatives;
- conducting privacy audits of records held by public sector organisations;
- considering applications for grants of authorisation made by public sector organisations to collect, use or disclose personal information in a manner that would otherwise contravene the Information Privacy Principles (**IPPs**);
- considering applications for extension of time periods relating to certain exemptions, e.g. the business information exemption (section 57 of the Act); and
- educating the public and public officers about FOI and privacy protection.

Since August 2018 the Office of the Information Commissioner (**OIC**) has been located within the Ombudsman's Office. Despite its location and utilisation of shared corporate support, the OIC remains an independent statutory office with a memorandum of understanding between itself and the Ombudsman's Office that covers sensible information sharing and referrals between the two offices.

The resources of the OIC are very limited. The Commissioner and Deputy have multiple roles (e.g., they are also Ombudsman and Deputy Ombudsman respectively) and so are able to contribute only part of their time to OIC functions. Apart from this, the OIC is principally comprised of one to two full-time positions. Necessary corporate support is provided by the Business Services Unit of the Ombudsman's Office. During this reporting period, an additional short-term position has been provided by Territory Families to assist the Commissioner in advising on privacy issues arising from the 360VOC data sharing project.[1]

[1] Discussed more fully at pp 25-26.

Freedom of Information

Annual statistics

New FOI applications received by all public sector organisations for the financial year 2022/23. An increase of 3% compared with 2021/22.

FOI applications finalised by public sector organisations for the financial year 2022/23. An increase of 10% compared to 2021/22.

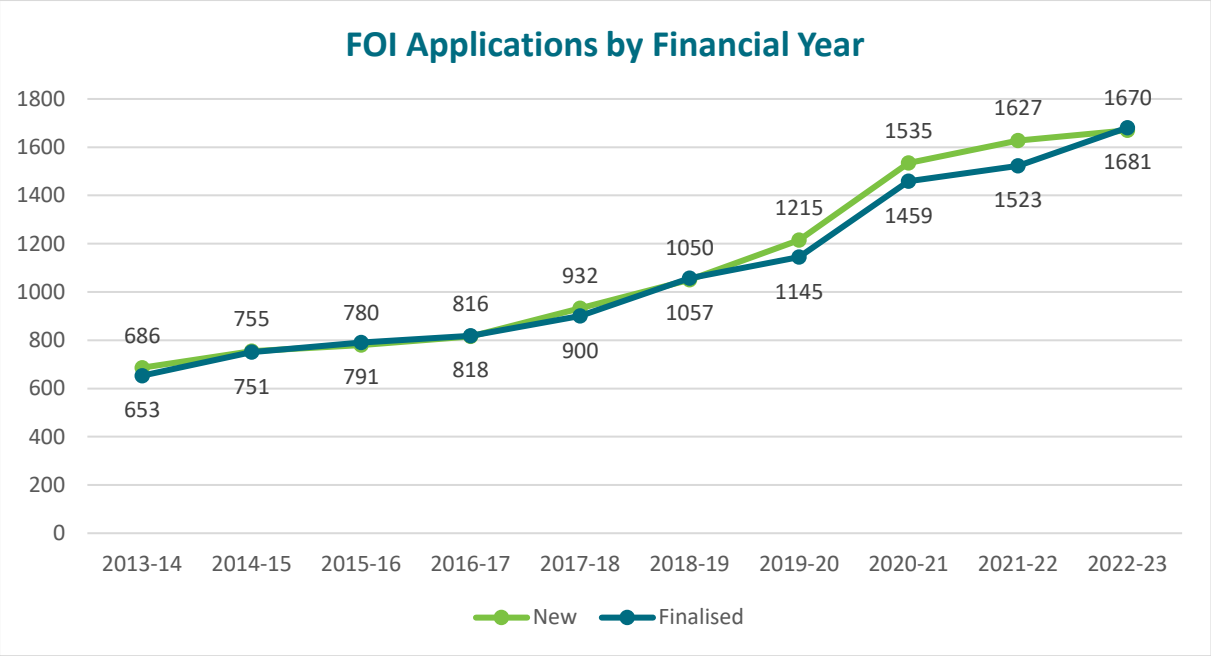
of new applications were for personal information about the applicant only.

of new applications were for non-personal information only.

of new applications were from political, media, activist or lobby groups.

FOI applications

The trend of annual increases in the number of FOI applications received by Organisations continued in 2022/23. Organisations are currently receiving twice the number of FOI applications compared to six years ago, often with little or no increase in resources.

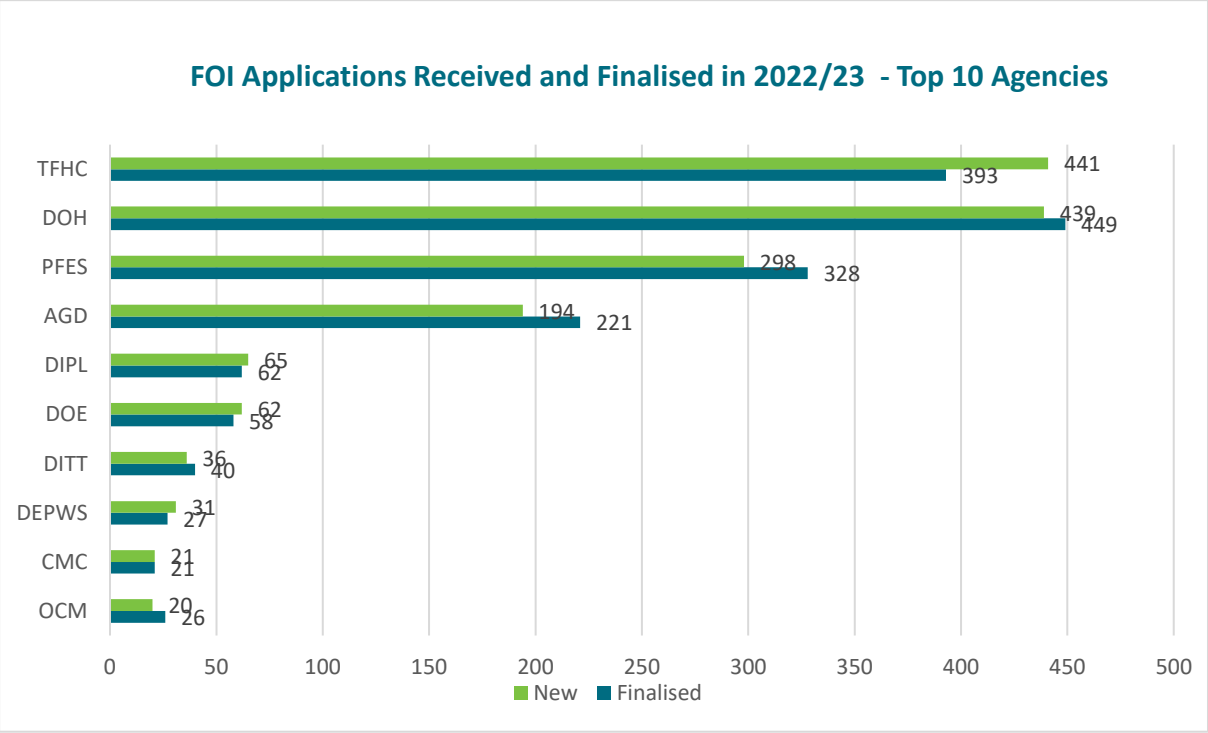


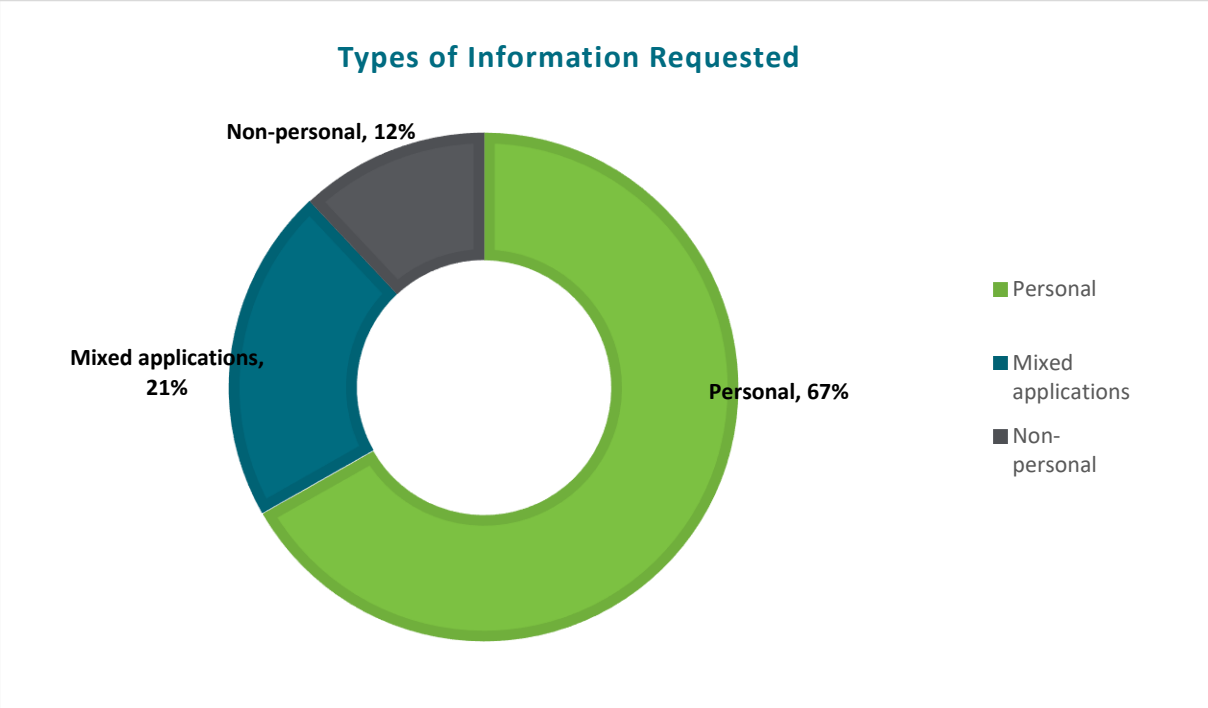
This year, the Department of Territory Families, Housing and Communities (**TFHC**) received more applications than any other Organisation, also experiencing the highest increase of 35% compared to 2021/22.[2] Since 2020/21, TFHC has experienced an 80% increase in applications received from 245 to 441. It has advised that the significant increase in FOI applications this year is partly the result of a large number of applications seeking information for the Stolen Generations Redress Scheme and the National Redress Scheme (Child Sexual Abuse). Further, it states a number of lawyers are electing to utilise the FOI process as an alternative to court subpoenas.

Some Organisations experienced a drop in new applications, including the NT Police, Fire and Emergency Services[3], the Department of the Attorney General and Justice[4] and the Department of Health[5].

Several Organisations managed to finalise more applications than they received (including applications carried over from the previous year).

[2] 327 in 2021/22 to 441 in 2022/23
[3] 345 in 2021/22 to 298 in 2022/23
[4] 249 in 2021/22 to 194 in 2022/23
[5] 474 in 2021/22 to 441 in 2022/23





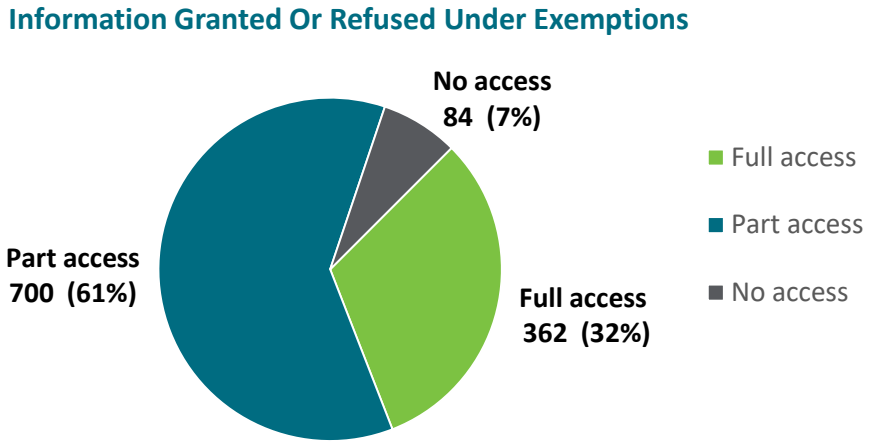
Application outcomes

The ultimate aim of the FOI process is to have an Organisation make a decision on whether, and to what extent, an applicant should be given access to particular information (the exemption stage). In broad terms, an Organisation may decide to refuse an applicant access to information sought on the grounds that providing access would be contrary to the public interest. The various grounds for refusing access based on an exemption are contained in Part 4 of the Act.

We will first discuss outcomes at the exemption stage before moving on to applications finalised on other bases.

Access refused because of an exemption

At the exemption stage, most FOI applicants are successful in getting all or some of the information they seek. In 2022/23, 7% of applicants (84 out of 1,146) were refused all information they sought on the basis of exemptions in the Act. This was higher than the 4% or 5% proportions experienced in previous years.



During 2022/23, the most widely used exemptions were those aimed at protecting:

- **the privacy of individuals** (section 56) – relied upon by 14 Organisations;
- **confidentiality** (section 55) – relied upon by 11 Organisations;
- **deliberative processes** (section 52) – relied upon by 9 Organisations;
- **commercial and business information** (section 57) – relied upon by 8 Organisations;
- **preservation of the system of justice** (section 49) – relied upon by 7 Organisations.

Making and progressing a valid application

An access application must meet the requirements of section 18 of the Act to be valid. It must be in writing, specify the name and contact address of the applicant and include sufficient details to identify the information sought. It must also be accompanied by the application fee (unless waived by the Organisation). Finally, before accepting the application, an Organisation must satisfy itself as to the identity of the applicant.

A valid application may be withdrawn by the applicant or transferred to another Organisation. An Organisation may also decide not to progress an application for other reasons, including:

- the information is already publicly available;
- a required deposit or processing fee has not been paid;
- the information sought cannot be identified or found or does not exist;
- the information is excluded from, or does not come within, the Act;
- providing access would unreasonably interfere with its operations.

There is a clear expectation that, as far as possible, Organisations will communicate with an applicant in a genuine effort to rectify any problems or deficiencies with an application in a manner that will enable the application to progress effectively. This may involve several rounds of discussion to clarify or refine its scope.

Even so, a large number of applications are finalised on these other grounds. Most prevalent among those during 2022/23 were approaches that did not meet the requirements for a valid application under section 18 (137), followed by cases where the information sought could not be identified or found or did not exist (130) and withdrawn applications (128).

A breakdown of these other outcomes by Organisation is set out at Appendix 2, Table 1A.

Review processes

If an applicant is not satisfied with the initial access decision they receive from an Organisation, they can ask for an internal review by another officer to allow the Organisation the opportunity to reconsider its initial decision.

Of the internal review decisions undertaken by Organisations during 2022/23, 70% confirmed the initial decision. The remainder (bar one withdrawn prior to finalisation) varied or revoked the first decision. Three decisions were referred back by the OIC under s 103(2) for a further review by the Organisation.

If an applicant is still not satisfied after an internal review, they can complain to the OIC. There is also provision for an Organisation to refer an application for internal review directly to the OIC as a complaint (section 39A referrals). Historically, some Organisations have chosen this path when they have had no one available or able to conduct an internal review or when they are confident that their first decision is the right one. However, most Organisations prefer to take advantage of the opportunity to reconsider their initial decision.

FOI matters by stage

	2021/22	2022/23
Total FOI applications received by Organisations	1627	1670
Internal review applications	33	40
Referred to OIC without internal review	0	0
Complaints to OIC after internal review	19	15

In 2022/23, 38% of internal review decisions became the subject of a complaint to the OIC. This is a decrease from the previous year, when 58% of internal reviews ended up as OIC complaints.

Noting the increase in FOI and internal review applications made to Organisations, the reduction in complaints made to our Office[6] is a welcome trend.

[6] See *FOI Complaints to OIC* at p.13.

We are aware of the difficulties faced by Organisations during the COVID-19 pandemic which caused staff shortages, re-prioritisation of 'non-essential' work and processing delays in many work units. Against this background, Organisations are to be commended for their overall performance in such challenging conditions. It is too early to tell, but it may be that a centralisation of FOI support services to a cross-agency FOI unit that occurred during 2022/23 is impacting positively on FOI decision-making. We will continue to monitor these matters.

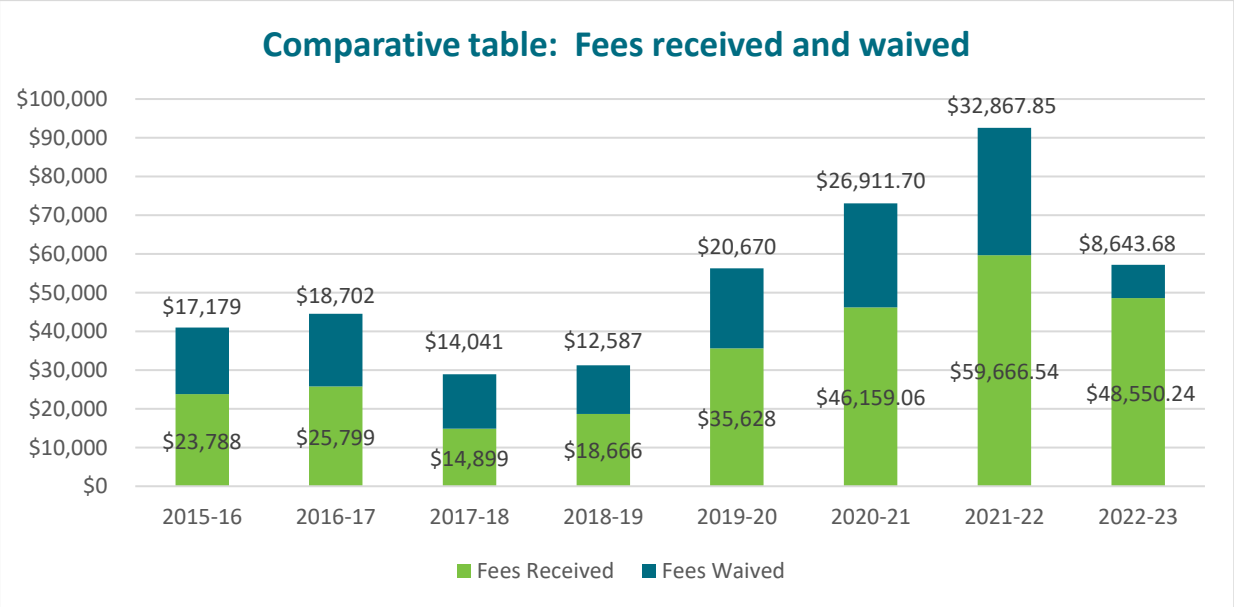
Application and processing fees

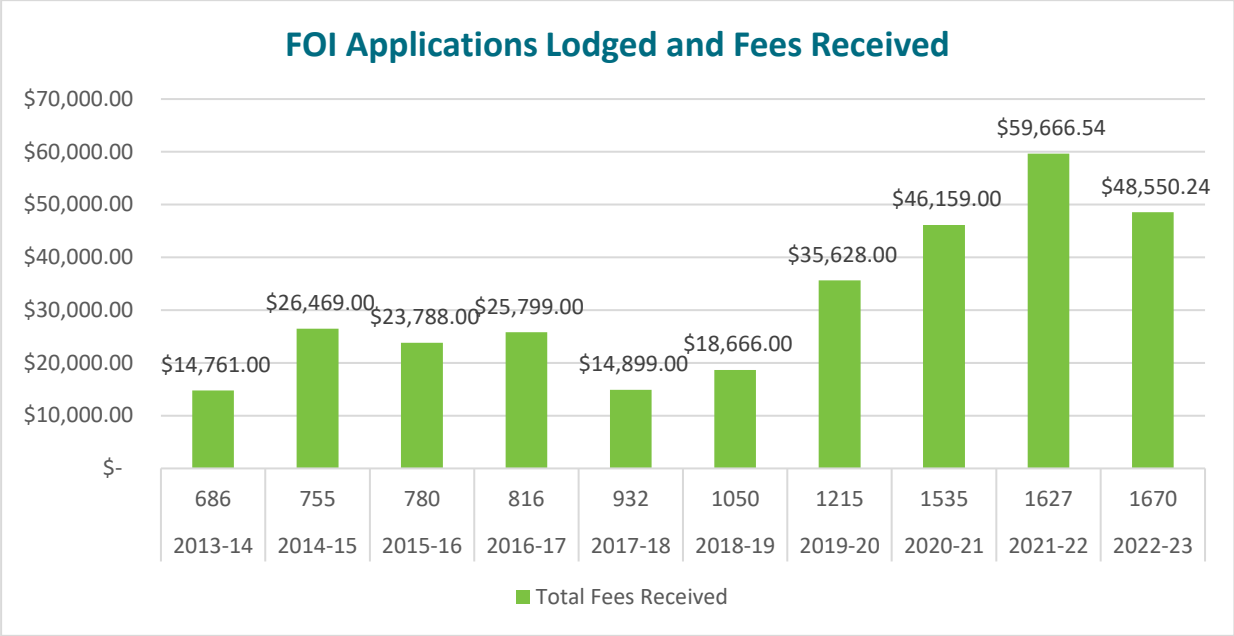
The Act provides for charging of application fees and processing fees. Similar to other jurisdictions, the maximum fees chargeable are set in legislation at a level well below that required for Organisations to recover the costs of administering the FOI scheme.

The fees are intended to act as a reasonable check on multiple and unnecessarily widely-scoped applications as they require an applicant to demonstrate their commitment to obtaining the information by assisting with associated costs.

No application fees are chargeable for requests for purely personal information and Organisations rarely charge processing fees for such requests. Historically, processing fees have seldom been charged if the request is small and straightforward on the basis that the resources required to collect fees in a large number of small matters would be uneconomic.

It is notable however that a considerably smaller proportion of fees were waived in 2022/23. Whether this reflects a change in policy within Organisations towards collecting fees remains to be seen.





A breakdown of fees received, reduced and waived by Organisation is set out at Appendix 2, Table 4 and 5.

FOI Correction applications

The scheme in the Act which allows people to apply to correct their own personal information (Part 3, Division 3) is seldom utilised.

No doubt difficult matters where Organisations are reluctant to amend the record are the ones that result in formal correction applications being made. The refusal to correct may be because the Organisation does not consider that there is an error on the file or they may consider that the error/wrong information is historical only. In circumstances where the disputed information is not removed, there is an option for a notation to be placed on the file to record the applicant's concern.

In 2022/23, seven applications to correct personal information were received by three Organisations, with two carried over from 2021/22.

Of the nine correction applications handled during the reporting period, none progressed to internal review.

The applications were dealt with by the Organisations as follows:

- one application resulted in the correction being made as requested;
- five applications were withdrawn; and
- three applications were refused.

Timeliness measures for agencies

At the end of the reporting period, Organisations are requested to provide statistical data regarding their compliance with legislative timeframes when finalising FOI applications within the 30 day statutory timeframe or any valid extension period.

The extension period makes allowance for reasonable delays in processing large applications or in consulting third parties if their personal or confidential information is intended to be released.

Data on this measure is collected annually as it provides a good indicator of how public bodies are managing an increasing workload and how the FOI scheme is working in terms of timeliness. The figures show that the majority of applications are finalised within 30 days[7]. Organisations reported 75% of initial access applications and 66% of internal reviews were finalised within 30 days. The proportion finalised within 90 days rose to 96% of initial applications and 90% of internal reviews. For internal reviews, this was a substantial improvement in timeliness compared with the previous year.[8]

Exemption certificates

The Chief Minister may issue an exemption certificate certifying that government information identified in the certificate is exempt for specific reasons set out in section 60 of the Act. We were not notified of any exemption certificates issued by the Chief Minister during 2022/23.

Challenging behaviours

No applications have been received this year for a declaration that a person is a vexatious applicant under section 42 of the Act. Even so, Organisations continue to contact the OIC seeking advice on appropriate methods for managing individuals whose conduct or demands appear to them to be unreasonable.

These types of situation need to be well managed as they can place considerable strain on everyone involved and require a reasoned, carefully implemented and staged approach to manage escalating behaviour. Our Office will continue to assist FOI officers and complainants with advice on maintaining a productive and workable relationship wherever possible.

Public resources to assist with management of challenging complainant conduct, include:

Ombudsman NT website: http://www.ombudsman.nt.gov.au/node/99/unreasonable-complainant-conduct, with links to NSW Ombudsman documents.

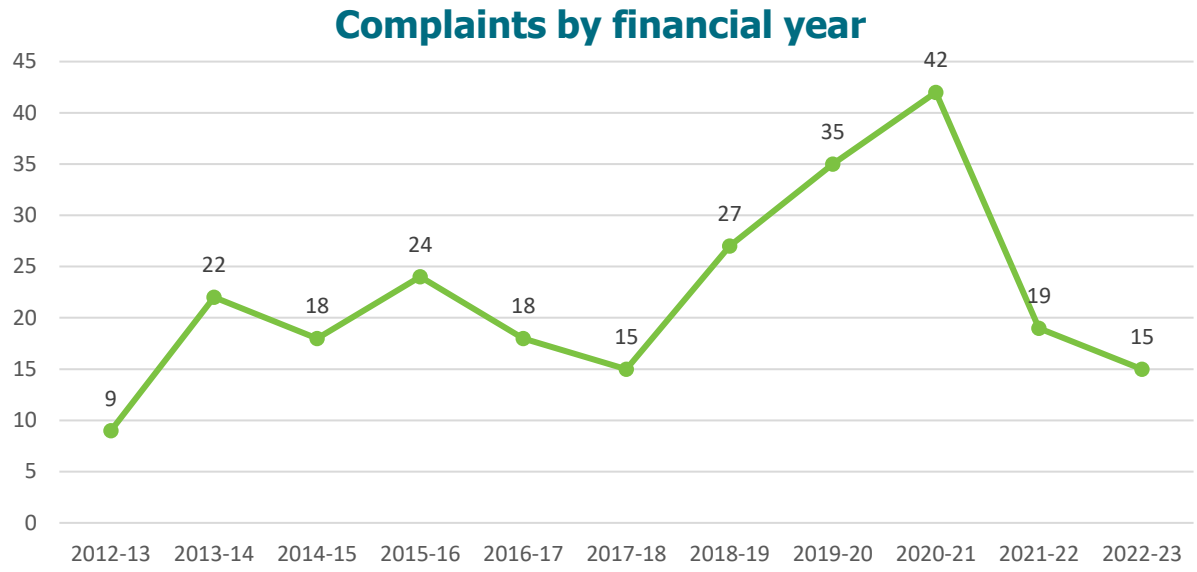
Victorian Ombudsman website: particularly the *Good Practice Guide to Managing complex complainant behaviour*, https://www.ombudsman.vic.gov.au/learn-from-us/practice-guides/.

Queensland Ombudsman website**,** *Managing unreasonable complainant conduct*, https://www.ombudsman.qld.gov.au/about-us/corporate-documents/managing-unreasonable-complainant-behaviour

[7] Proportions are based on figures provided by Organisations.
[8] In 2021/22, 50% of internal reviews were finalised within 30 days and a further 21% within 31 to 90 days.

FOI complaints to OIC

The number of FOI complaints received by the OIC again decreased this reporting period. The OIC received 15 FOI complaints, a reduction from 19 in 2021/22. This is a significantly lower number of FOI complaints compared to the peak of 42 received in 2020/21. The reasons for the reduction are difficult to identify but it may have been contributed to by the creation of a centralised FOI Unit to assist NTG Organisations.

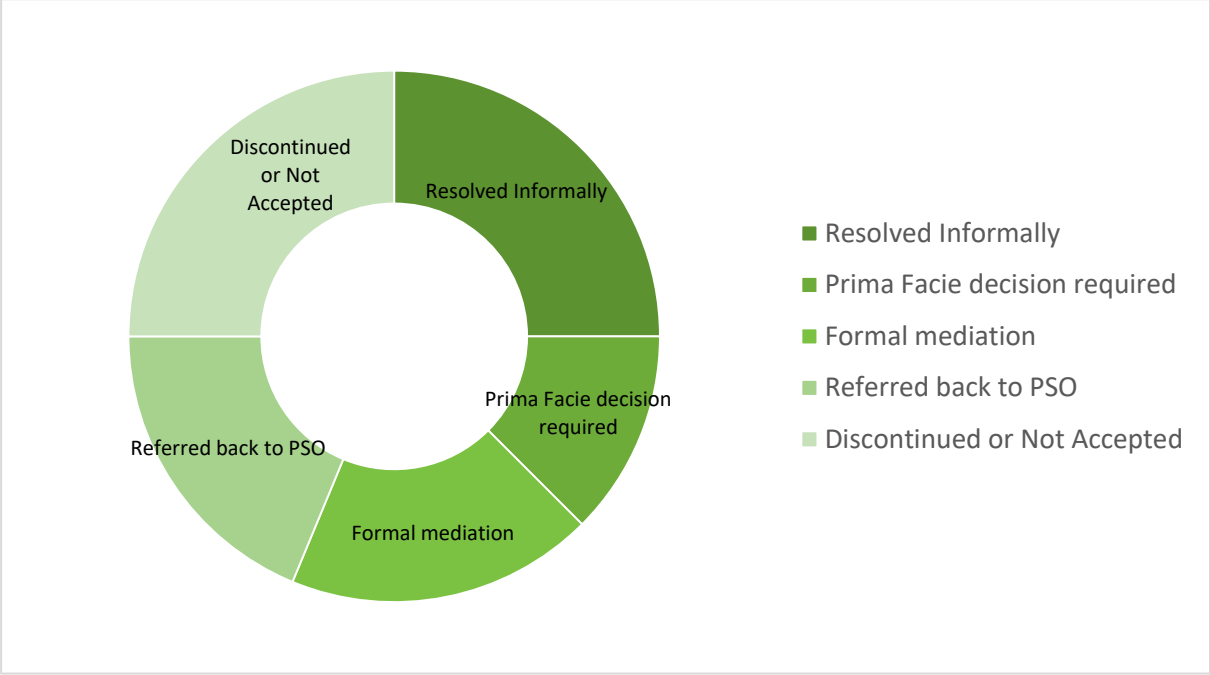


The table below lists the FOI complaints handled by our Office during this reporting period, by Organisation (including 19 carried over from the previous year).

Organisation	New Complaints	Carried Over	Finalised	Open at EOY
AAPA	1			1
AGD	4	4	5	3
CDU		1	1	
CoD	1			1
DCMC	1			1
DEPWS	1	2	1	2
DIPL	1	1	2	
DITT	1		1	
DoE		7	3	4
OCM	4	3	1	6
PFES	1	1	2	
TOTAL	**15**	**19**	**16**	**18**

Note: See Appendix 2 for the full names of abbreviated public sector organisations referred to in the table.

During the year, 15 complaints were finalised, with the following outcomes.



Two complaints finalised during the reporting period were referred to the NT Civil and Administrative Tribunal (**NTCAT**) for hearing.

Timeliness

Timeliness in complaint management in recent years has been affected by an increase in complaint numbers and/or other functions undertaken by the OIC within finite resources. We have also needed to accommodate the personal circumstances of a number of complainants who were unable to participate in a timely manner for health and other reasons.

A decrease in new complaint numbers during 2022/23 provided an opportunity to finalise a number of older complaints carried over from the previous reporting period.

During 2022/23, timeliness outcomes for FOI complaints were:

- 44% finalised within 0–6 months
- 13% finalised within 6-12 months
- 43% finalised after 12 months or more.

Complaint case studies

Purely statistical, technical, scientific or factual material

The ‘Cabinet in Confidence’ class exemption is based on the need to preserve collective ministerial responsibility. It is an exception that exists in all Australian jurisdictions and is a class exemption that has been accepted by the Australian Law Reform Commission as justifiable. ‘Collective ministerial responsibility’ means that we have a system of government where Ministers are able to debate freely in secret, and then present a united view on what the Government will do. However, there are some limitations on the information that can be refused under this exemption.

In this particular matter, *A* submitted a FOI request to the Respondent to obtain a copy of an independent review report commissioned by the Government to investigate an incident that occurred in one of the Respondent's facilities. The Respondent refused access under section 45(1)(a)(i) of the Act because the information sought was brought into existence for submission to Cabinet. *A* lodged a complaint with our Office following receipt of an internal review decision from the Respondent upholding its original decision.

A delegate for the Commissioner conducted an investigation and requested additional information from the Respondent, which in the delegate's view confirmed that the report was created for Cabinet consideration. The delegate noted however that some parts of the report appeared to contain purely statistical, technical, scientific, or factual material that might be released as it would not disclose Cabinet deliberation or decision-making.

The delegate informed the Respondent of this view and proposed an early mediation between the parties. After mediation, a redacted copy of the report was released by the Respondent, excluding any information that they considered was exempt under the Cabinet in Confidence exemption. *A* subsequently withdrew the complaint and the file was closed.

Scope negotiation

There is an obligation on Organisations to contact the applicant and negotiate the scope of an application if they consider it to be unclear or too broad. In this case, the attempts made by the Organisation (the Respondent) to negotiate and reduce the scope were considered on review to be insufficient. Further, before refusing an FOI application on the grounds that it is so broad that processing the application would unreasonably interfere with their operations (s 25 of the Act), the Respondent must take meaningful steps to estimate the scope of the search required so that their decision is evidence-based and supportable. That did not happen in this case.

B lodged an FOI application but the Respondent decided that the scope of the application was too broad. Two attempts were made by the Respondent to negotiate the scope and on each occasion, counter offers were proposed by *B*. In response to *B*'s second counter offer, the Respondent stopped negotiating and instead issued a Notice of Decision on the grounds that processing the application would unreasonably interfere with its operations (s 25 of the Act). *B* applied for an internal review of the decision and stated the he was under the impression that they were still negotiating the scope.

The Respondent conducted an internal review of its decision and decided to process the application using the second scope terms earlier proposed by *B*. Rather than the scope being too large to be processed, the Respondent found there was no relevant information. Consequently, the application was refused under s 27 of the Act (i.e. information cannot be found or does not exist).

B lodged a complaint with the OIC. A delegate for the Commissioner provided a preliminary view to the Respondent that *B* had a prima facie case for the following reasons:

- the Respondent at first instance did not undertake a sufficient search of departmental records before refusing the application on the grounds of unreasonable interference (s 25 of the Act); and

- upon review, instead of liaising with *B* when a search was undertaken and no information was located, the Respondent again refused access without first consulting with *B* to ensure procedural fairness. Having first been told the search was too large to undertake and later being told that there were no documents, *B* was left feeling frustrated and skeptical of the outcome.

The OIC recommended that the Respondent further review the application and genuinely consult with *B*. The Respondent agreed and the OIC referred the matter back to it under s 103(2). As a result, additional searches for the documents sought were undertaken using an agreed broader scope, but no further information was located. The Respondent provided *B* with a thorough explanation of what searches had been undertaken and the complaint was finalised.

Extension of time

In 2022/23, I finalised one application from a third party objector company to extend the time for exemption of information relating to its operations.

In *Re Various Applications Under the Information Act 2002* [No. 2] [2020] NTCAT 2, the NTCAT determined that a third party objector can only pursue an exemption-related objection to disclosure on the basis of an exemption with respect to which it was entitled to be consulted under section 30 of the Act. This meant the objector was limited to contending for exemption under section 57(1) of the Act, the commercial and business information exemption.

However, there is a five year time limit on this exemption and the third party objected to disclosure of some information that was created or obtained by the Organisation more than five years ago. The Act provides for extension of that timeframe by the Information Commissioner in certain circumstances, so, in order to have any prospect of sustaining a claim to exemption, the objector needed to apply to me for an extension.

In a previous decision, I made the following general comments regarding the application of section 57(6), which I maintain:

> *The power to extend a time limit should be viewed in the context of the elements necessary to establish the exemption but is not limited to those elements.*
>
> *The provision does not require an application to be made prior to the expiry of the 5 year period. In practical terms, the only time a third party is likely to be concerned about the limitation is when they are in the process of responding to an access application. This may arise at any time, potentially well after the five year limit has expired. If an application was required to be made prior to expiry, the Commissioner might be subject to countless applications from businesses seeking to preserve their rights, to guard against the comparatively rare prospect that an access application might be made in the future.*
>
> *There is no specific provision for an application process but a clear statutory intent that the matter can be raised with the Commissioner. While one might ordinarily imagine such an issue would be raised in the course of initial consultations or a complaint to the Commissioner, there is no statutory bar to the matter being raised at any time.*

The information in issue related to a communication that was sent to staff of an Organisation, purportedly from the third party objector. At face value, the communication might be construed as evidence of some impropriety by the third party. However, the third party contended that the communication was fabricated to appear that way.

At the time of the communication, the third party acted quickly to address it with the Organisation, providing cogent evidence in support of its contention. The Organisation considered this evidence, consulted other authorities and obtained legal advice, before deciding not to take further action in relation to the communication.

I analysed the strength of the contention that the information in issue would continue to qualify for exemption under section 57(1) if an extension were to be granted. I reviewed the information and the submissions of the third party, concluding it was arguable that disclosure of any of the information in issue at the time of my decision would be likely to expose the third party unreasonably to disadvantage. I ultimately decided that it was in the public interest to grant an extension beyond the usual five year period.

I noted that the strength of the adverse impact on the third party will diminish over time, therefore deciding the extension should be limited. I extended the application of the exemption provision in relation to the information in issue for five years.

This was not a finding that the information was exempt but it did allow for the possible application of section 57(1) beyond the five year period.

NTCAT FOI proceedings

Following a decision finalising an OIC complaint, an aggrieved party can apply to the Commissioner to refer the decision to NTCAT for hearing. In such cases, the OIC prepares a referral report to NTCAT and, in some cases, participates in the Tribunal proceedings. Selected NTCAT decisions are published on the Australian Legal Information Institute (AUSTLii) website[9].

In this period, two FOI matters were referred to NTCAT, with one matter finalised by an NTCAT decision. The remaining matter is still before NTCAT. Set out in the below case study is a summary of NTCAT's reasons for decision.

Record cannot be located (unpublished)

C sought specific information from the Respondent about an incident in 2016 involving him, including reports, request forms and outcomes. While certain information was provided to *C*, one specific document was not included. *C* requested a review of the initial decision, identifying the document he wanted. Subsequently, an internal review was conducted by the Respondent, and they advised *C* that they were unable to locate the folder containing the relevant document.

C lodged a complaint with the OIC stating that there should be a copy of the document on their personal file with the Respondent. During investigation by the OIC, the Respondent provided search declarations demonstrating searches that were made by the Respondent to locate the relevant document and a further explanation as to why the document could not be located. The OIC provided a preliminary view to *C* that the Respondent had taken all reasonable steps to locate the document however it could not be located. The complaint was dismissed by the OIC on the basis that there was not sufficient prima facie evidence to substantiate the complaint.

[9] http://www8.austlii.edu.au/cgi-bin/viewtoc/au/cases/nt/NTCAT/2015/

During the proceedings before the Tribunal, *C* expressed doubt about the genuineness of the attempts made to locate the document and alleged corrupt conduct. The Tribunal noted that *C* did not provide evidence to support these claims. The Tribunal also noted that the assertion of corruption was not part of the initial complaint to the OIC.

The Tribunal concluded that the decision to dismiss the complaint by the OIC was correct based on the information available. It was established that reasonable searches had been conducted, but the requested document could not be located.

The Tribunal remarked that while section 27 of the Act does not amount to an exemption under the Act, it constitutes a basis for refusal to provide the information if in fact the information sought cannot be found. In this case, the Tribunal found no prima facie case to challenge the constructive refusal.

Ultimately, the Tribunal confirmed the OIC's decision and dismissed the complaint.

Privacy Protection

All NT public sector organisations are bound by the Information Privacy Principles (**IPPs**) in the Act in how they collect, use, disclose, secure and destroy personal and sensitive information that they hold. The OIC is the 'privacy watchdog' for the NT public sector. The OIC investigates and mediates privacy complaints made by individuals against Organisations in circumstances where the Organisation has been unable to resolve the complaint.

A complainant is first required to approach the Organisation and give it a reasonable chance to resolve or rectify the matter complained of before coming to the OIC.

Attempts are made by our Office to resolve privacy complaints at an early stage. Mediation allows parties to have open and frank conversations about an alleged breach of privacy and exchange information in a protected setting. On occasion, this exchange of information may alter each party's perception of what occurred and/or help them understand the other's point of view. While some settlements are confidential[10], outcomes achieved at mediations this year included payments of compensation, letters of apology and agreements by Organisations to undertake particular actions.

If matters don't resolve through the complaint processes within our Office, the individual can seek referral to the NT Civil and Administrative Tribunal (**NTCAT**) for a decision as to whether or not a privacy breach has occurred and whether orders should be made to prevent ongoing action, rectify the breach or compensate the complainant.

The OIC also allocates significant resources to providing advice to Organisations on privacy protection either in their day to day work or when they are implementing new initiatives. In addition, the OIC provides education and advice to the public on their privacy rights under the Act. This financial year has been particularly busy in the privacy space as we continue to support Organisations and Territorians in ensuring personal and sensitive data is protected.

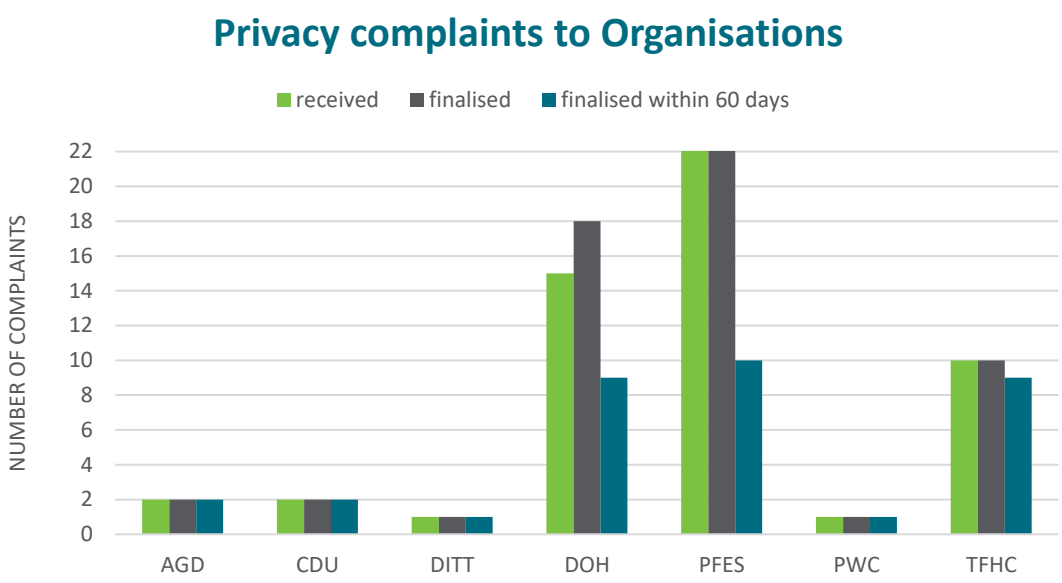
Privacy complaints to Organisations

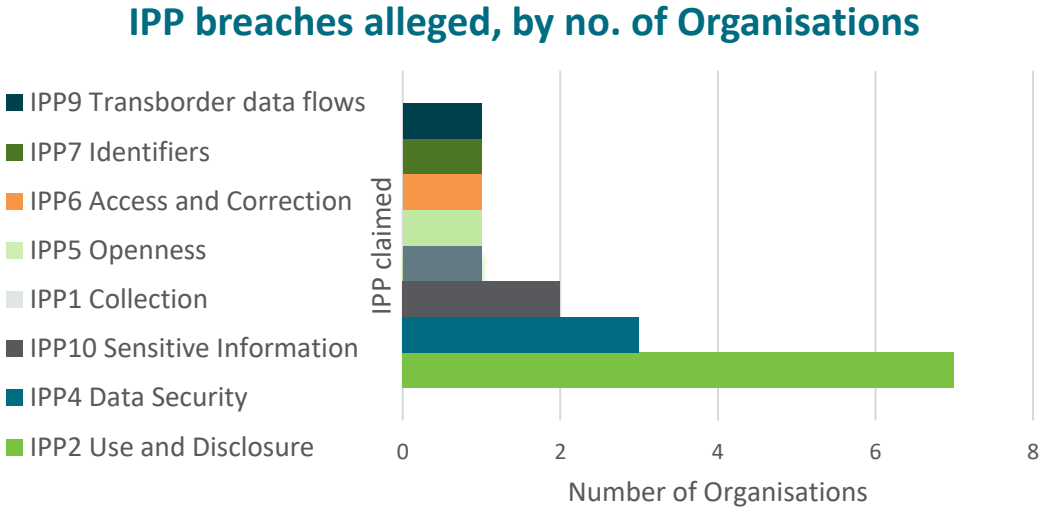
Legislative reporting requirements for Organisations in relation to privacy complaints they receive are not as structured as for FOI applications. In an attempt to gain insight into the management of privacy complaints by Organisations, our Office now seeks additional information from them on an annual basis.

During 2022/23, Organisations reported the following:

- A total of 55 new privacy complaints were reported as received by 7 Organisations, with 11 carried over from 2021/22 (i.e. 66 complaints handled in the reporting period).
- These privacy complaints alleged breaches of various IPPs, including collection of personal information (IPP 1), use and disclosure of personal information (IPP 2), information security (IPP 4) and access and correction (IPP 6).
- Organisations finalised 58 out of the 66 privacy complaints handled during this period, with 34 complaints finalised by Organisations within 60 days.
- Police and Health received the most privacy complaints.

[10] Mediations are on occasion adjourned to allow the parties' time to enter into a private agreement which may include confidentiality provisions.





Remedies

This year, remedies adopted in resolution of privacy complaints included:

- General change to agency practice or systems
- Compensation
- Apology
- Agency refrain from repeating or continuing to do an act
- Offer of staff training and commitment to educate
- Decision to take disciplinary action against the wrongdoer
- Offer of further discussion with the complainant about privacy-related concerns
- Agreement to add a note on complainant file
- Correction or deletion of personal information about the complainant held on the Organisation's files.

Privacy complaints to OIC

If a complainant is dissatisfied with the action taken by the Organisation on their privacy complaint, they can complain to the OIC. The OIC received seven new privacy complaints during 2022/23.

Organisation complained about	New complaints	Carried over	Finalised	Open at EOY
AGD	1			1
CDU	1		1	
DOE		1		1
DITT	1		1	
DOH	3		1	2
PWC		1		1
PFES	1		1	
TOTAL	**7**	**2**	**4**	**5**

Note: See Appendix 2 for the full names of abbreviated public sector organisations referred to in the table.

Four privacy complaints were finalised during 2022/23 — two were resolved informally and two were ultimately discontinued/not accepted by the OIC.

Timeliness

This year, timeliness was significantly impacted by the need to accommodate the personal circumstances of a number of complainants, limited OIC resources and competing demands that often caused delays in receiving responses from complainants and Organisations.

All four privacy complaints completed this year were finalised within 6 months.

Privacy/Data breach notification

There is no legislative requirement on Organisations or public officers to advise the OIC when there has been a data (privacy) breach but some Organisations choose to inform us and seek our advice. Organisations reported eight data breaches to our Office in 2022/23.

The breaches reported to OIC were of varying levels of seriousness and occurred in both large and small organisations and in various parts of the Territory. Most appear to have been due to human error but it is pleasing to see that in each reported case, they were taken seriously by the Organisations, and have led to changes to policies and practices and staff training.

The reported data breaches included:

- *Incorrect email recipient*: Staff member A inadvertently forwarded a work email containing another's personal information to a personal contact. Staff member A immediately advised senior executive of the error and confirmed the personal contact had deleted the email.
- *Incorrect email recipient*: Contractor A inadvertently sent a copy of a work email for staff member B to an incorrect recipient outside the Organisation. Staff member B immediately contacted the recipient and sought confirmation of deletion of the email. Staff member B also notified contractor A of the error.

- *Pre-filled application forms*: Clients received pre-filled application forms of third parties who were unrelated to the client due to a printing error. In 2021/22, a similar notification had been reported to us, which was attributed by the Organisation to human error.
- *Incorrect attachment sent*: Organisation C sent an attachment disclosing to the recipient the name and mobile number of Organisation D's staff member. Organisation D confirmed the staff member no longer worked there and the mobile number was Organisation D's asset, therefore the risk of harm was low. OIC recommended that Organisation D contact the affected party regardless and explain the steps taken to address breach.
- *Disclosure of customer details to third party*: Staff member C disclosed Client A's name and address to Client B. Client B tracked down Client A and the police were required to be called. Client A was upset with the Organisation for disclosing their personal information. The Organisation acknowledged a privacy breach and took steps to review their processes and discuss the matter privately with Client A.
- *Loss of file*: Client requested a copy of their records from the Organisation, however they were unable to locate them. The client made a privacy complaint to the Organisation and the Organisation concluded they had contravened the Act. The Organisation made recommendations to the relevant area in relation to this matter and confirmed it was dealing with the privacy concerns directly with the client.
- *Cyber hacking incident*: The system of a third party consultant which held information from a number of Organisations (which may have included personal information of clients of those Organisations) was hacked. The nature and extent of the information stolen is under investigation. The consultant is working with the Organisations that may be affected.
- *Inadvertent full access to customer records*: A staff member (who does not handle client records) had been granted full access for approximately 18 hours to client information following a system error. Upon becoming aware of this error, changes were made and normal access was restored. There was no evidence that information disclosed was accessed/distributed/acted upon outside the Organisation.

As in previous years, some notifications and enquiries related to breaches that might not have occurred had there been better processes or greater staff training within the Organisations.

When notified of a privacy breach by an Organisation, this Office provides advice about options for action and possible steps to minimise the risk of harm to the individuals affected. It is most important that affected individuals are made aware of any serious breach and that they are aware of their right to make a privacy complaint should they wish to do so. We also work with Organisations to minimise their future risk and to improve their privacy protection and staff training.

There has rarely been a time when public concern about the protection of privacy has been more prominent. Recent cyber hacks have heightened public awareness and there is a real appetite on the part of people to know about how government and businesses are handling their data and when problems arise. With that in mind, it is important for Government to act to ensure a fair and consistent approach to data breach reporting.

The OIC has worked with NT Government officers over time to advance development of a whole of government approach to data breach reporting but there is, as yet, no mandated system.

A number of Australian jurisdictions, including the Commonwealth and NSW, have legislative mandatory data breach reporting requirements. These provide clear guidance for agencies on when breaches should be reported to the relevant oversight body and to affected people. They also provide for regular public reporting on notifications of serious breaches. They provide a standard which promotes organisational and public understanding of when reporting is required.

There appears to have been no discernable progress in the development and finalisation of a Data Breach Plan and Policy for NT Government Organisations during 2022/23. This is regrettable, particularly when there is a momentum for greater information sharing of personal information between Organisations and with other external bodies.

The introduction of a robust mandatory data breach notification system, consistent with other Australian jurisdictions, would be a significant step in protecting the privacy of Territorians.

Privacy Case Studies

Disclosure of sensitive information at a staff event

D was a former employee of the Respondent. Shortly after their resignation, *D* was notified by one of their former co-workers that a senior executive from their organisation had disclosed their sensitive information at a staff event. *D*'s sensitive information was disclosed to an audience of several hundreds and was livestreamed via social media.

D lodged a complaint alleging a privacy breach by the Respondent. Following investigation, the Respondent agreed that it had breached *D*'s privacy and offered *D* compensation. *D* was dissatisfied with the Respondent's response and lodged a complaint with our Office.

During investigation by the OIC, *D* raised several outcomes they were seeking, including a reinstatement to another permanent full-time position, an apology directly from the senior executive who had breached their privacy and compensation. The OIC advised *D* that the first outcome was not a remedy available under the Act, however the OIC raised it with the Respondent.

The Respondent declined to provide the first outcome as the employment termination was not directly related to *D*'s privacy complaint. However, the Respondent provided an apology from the relevant officer and the matter was resolved upon agreed terms.

The power of mediation

At the time of making a privacy complaint, *E* was employed by the Respondent. Whilst employed, *E* sent an email in their capacity as a private citizen to the relevant Minister (whose portfolio included the Respondent Organisation) raising sensitive issues impacting on many families (including *E's* family) and querying the adequacy of staff resourcing within the Organisation to deal with the issues.

The email, including *E's* sensitive information, was sent from the Minister's office to the Respondent and further provided to some senior managers for consideration of next steps.

When the initial response from management appeared most unsupportive of *E's* actions in contacting the Minister, albeit in a private capacity, *E* resigned from employment with the Respondent on the basis that a mutual relationship of trust and respect no longer existed between them.

E also lodged a breach of privacy complaint questioning why their letter to the Minister had been provided to senior managers and why it was perceived that *E* was the wrongdoer.

After a period of delay in the Respondent providing a formal response to *E's* privacy complaint, *E* approached our Office. After investigation, a delegate of the Commissioner decided that there was sufficient prima facie evidence to substantiate the complaint and the matter was referred to mediation, which was ultimately successful in resolving matters.

An important comment to make regarding mediation:

In this case, the presence of the appropriate Respondent representative at mediation assisted the process, as there was a mutual respect evident between *E* and the representative. Further, the Respondent representative actively listened to *E* and maintained a compassionate and empathetic approach to issues raised by *E*, ultimately leading to a confidential settlement between the parties.

Other OIC operations

The past two years have seen a number of NTG Organisations upgrading their digital systems to better service Territorians and streamline organisational functions. The OIC has limited involvement in the technical aspects of the system upgrades but we continue to make ourselves available to assist agencies to ensure that new technologies are respectful of each individual's right to privacy and compliant with the relevant IPPs in the Act.

Child protection data access agreements

Throughout the reporting period, my Office has provided advice to Territory Families on a new technological solution to assist them in keeping vulnerable children safe. The information sharing envisaged by this new digital solution will be supported by Data Access Agreements (**DAAs**) that authorise provision of information to Territory Families. The DAAs are authorised by changes to the *Care and Protection of Children Act 2007*, made in early 2022. The amendments require the CEO of Territory Families to consult with my Office when entering into a DAA. An additional resource (a senior policy officer) has been provided to the OIC to assist with this project.

In my last Annual Report, I provided an extract from correspondence to the CEO of Territory Families that remains relevant to this project:

> *There is no question that part of government's role in protecting a vulnerable child is to ensure that systems exist for the sensible sharing of information between agencies and others with a legitimate interest in the safety and welfare of the child. Throughout my time as Information Commissioner, I have strongly supported responsible information-sharing and encouraged proposals that provide for it. Similarly, the Coroner raised concerns about poor information sharing in a recent inquest and noted the earlier recommendations in the Little Children are Sacred report that addressed this issue. The Coroner's recommendations included that 'the Multi-Agency Community and Child Safety Framework be legislated so as to ensure mandatory cooperation, coordination and information sharing in a timely manner.' … I am supportive of the Coroner's comments and his recommendation to improve information sharing. …*
>
> *The concepts of responsible information-sharing concerning 'child safety and wellbeing' and the need for privacy protection are closely linked and are not mutually exclusive. If a child's safety is at risk, then a robust sharing of information is vital. … Wellbeing, however, is a very broad term that is defined in the Oxford dictionary as 'the state of being or doing well in life; happy, healthy, or prosperous condition'. … Wellbeing includes an individual's right to privacy unless there is good reason otherwise. …*
>
> *There is … danger in legislation that oversteps the mark in terms of ostensible legal authority to collect, leading to families, non-government organisations and indeed professionals within government agencies, failing to record information or recording minimal information in case it is sought under the legislation. This could lead to drying up of available information which would be in no-ones interests.*
>
> *As I have stated on numerous previous occasions, it is important that stakeholders be engaged and supportive of the undoubtedly valuable policy aims of the legislation, if information-sharing is to be truly effective.*

From the outset, the position of my Office has been to accept the underlying importance of reasonable information sharing in this context, while robustly testing whether the scope and mechanisms for such sharing exceeds what is reasonably required to meet the policy aims of Government.

The technological solution will involve automated provision to Territory Families of a range of specified personal information held by a range of agencies, relating to children who have involvement with Territory Families, including those in their lives who are considered to be a 'close connection.'

This is a very broad information sharing scheme, involving information about a substantial number of Territory families, held by bodies as diverse as NT Police, Health, Education, Courts and Correctional Services. The intention behind obtaining so much information is to provide a 360 degree view of the life of a child for use by Territory Families in making decisions about their care and protection. The information will be available to Territory Families authorised users through the CARE System, the operational child protection system. At the time of preparing this report, work is still continuing on the technological solution, known as the 360View of the Child (**360VoC**) Solution.

Any cross-agency information-sharing agreement takes collaboration and a clear, common goal to ensure the best outcome for stakeholders. Throughout 2022/23, relevant agencies have spent considerable time and effort working with Territory Families, the Department of Corporate and Digital Development (who are designing and building the technological solution) and my Office to reach agreement on what personal information should be available to Territory Families, who will have access to it and how it will be protected.

During 2022/23, I made one Grant of Authorisation under section 81 of the Act to assist the relevant Organisations in the technical build of the 360VoC Solution by allowing the development team to access limited personal information from each participating Organisation to facilitate matching information from disparate IT systems. The access approved by the Grant was limited to information judged to be required to test the software and advance the technical build. Safeguards were put in place to ensure that the personal information accessed during this development stage is kept safe and secure. Broader stakeholder consultation is intended to occur before the 360VoC Solution goes live.

Domestic & family violence information sharing review

Amendments to the *Domestic and Family Violence Act 2007* (the **DFV Act**) were introduced to assist government agencies and non-government organisations involved in supporting victims and families impacted by family violence to share information with the aim of keeping them safe. The information sharing amendments are contained in Chapter 5A of the DFV Act.

Section 124U of the DFV Act requires the Information Commissioner to review the first 2 years of operation of this Chapter, and later to review the 3rd to 5th years. Each review must include consultation with the Minister and with information sharing entities (**ISE**s). It must also consider any adverse effects of this Chapter. The Information Commissioner's report to the Minister may include any recommendations on any matter addressed in the review. It is required to be tabled in Parliament.

Extensive stakeholder consultation has occurred and a report is anticipated to be delivered to the Minister in the near future.

General enquiries

The OIC receives enquiries from Organisations and the public about the FOI scheme and privacy rights and obligations.

Questions from members of the public commonly relate to:

- which Organisation to lodge an FOI application or privacy complaint with;
- the process and procedure for making an application or privacy complaint, requesting a review of an Organisation's decision or making a complaint to the OIC;
- the wording required for an application; and
- the payment of fees.

Enquiries from Organisations are often more complex and may involve such matters as:

- seeking the Commissioner's position on particular wording in the Act,
- seeking information about legislative exemptions that may form a basis for a refusal of a request for access to information;
- clarifying what consultation is required with an applicant in negotiating the scope of an FOI application;
- seeking assistance in reaching a mediated settlement in a privacy complaint;
- seeking advice on how to manage a privacy/data breach;
- seeking advice on how to undertake a privacy impact assessment; and
- seeking other advice on the complaint process.

Our Office provides individuals and Organisations with guidance on the Act and the IPPs. Where appropriate, we refer enquiries to the information unit of the relevant Organisation or we engage with the Organisation to assist the individual.

In 2022/23, the OIC received a total of 263 general enquiries:

- 182 related to FOI matters;
- 65 related to privacy matters; and
- 16 related to other matters.

Often these enquiries relate to simple matters. Some enquiries however are far more complex, involving consideration of jurisdictional issues or interpretation of the Act.

Advice and comment on policy and legislative changes

A key component of the OIC's work is to provide expertise, advice and commentary to Organisations on their policy developments and initiatives. The OIC cannot provide legal advice, however we regularly provide guidance and support to Organisations during the development and review of their practices, policies and legislation. We also provide specific guidance on new initiatives, including the need for Organisations to conduct a privacy impact assessment.

The majority of requests for advice relate to privacy issues. The amount of time spent providing advice fluctuates depending upon the initiatives being undertaken by Organisations and the level of assistance they require from the OIC.

During 2022/23, the OIC provided a record 2,086 hours of advice to Organisations and other stakeholders on matters relevant to the Act. Much of this time was spent providing advice to Organisations on Data Access Agreements and the 360VoC Solution. Considerable time and resources were also spent on assisting with the initial consultation process and other preliminary steps for a review of the FOI, privacy and record management provisions in the Act.

Specific advice was also provided to Organisations on a range of topics, including:

- Privacy considerations when implementing a process for banning individuals from public transport and what should be covered in a public bus CCTV privacy policy;
- Privacy considerations for a review of processes for collection and storage of sensitive information about public officers and employment;
- Responsible and appropriate information sharing within an Organisation where various work units undertake different work under separate legislation;
- Administrative release of personal information to individuals and the need for guidance to staff and stakeholders about instances when information will be released;
- Public information that an Organisation should have available about the way the Organisation manages personal information;
- Managing a privacy data breach and preventative measures to avoid future occurrences;
- Consultation and advice on protocols for access to NT Government records to facilitate applications to redress schemes.

Awareness, education and training

During 2022/23, the easing of COVID-19 restrictions meant that our Office was able to re-engage with the community in person and also resume facilitating face to face FOI training for NTG officers.

Community Engagement

In July 2022, the OIC sent two staff members to Alice Springs to engage with a range of stakeholders and spread awareness to the general public about the role of our Office. In June 2023, the OIC made a similar visit to stakeholders in Katherine.

The OIC has also joined with the Ombudsman's Office on various outreach and community engagement activities including two Seniors Expo events hosted by COTA in July 2022 and May 2023.

Training for NTG agencies

In October 2022 and April 2023, the OIC assisted with the facilitation of FOI Training conducted by an external FOI expert. The training was attended by approximately 40 participants from various NT government agencies attending in person.

The first half of the training session provided an overview of the Act, including information and records management requirements, FOI processes, exemption provisions and charges. The remainder of the session focused on decision-making and applying the exemption provisions of the Act. There continues to be an ongoing demand for the provision of this training.

Privacy Awareness Week

Privacy Awareness Week (**PAW**) is held annually each May, highlighting the importance of protecting personal information for the public and officers from government agencies. Although this year there was no forum held in the NT, the OIC updated its website for PAW, promoting the theme *"Back to Basics",* highlighting the importance of keeping personal data safe in the ever-evolving technological landscape.[11]

International Access to Information Day

Annually on 28 September, the OIC celebrates International Access to Information Day, also known as Right to Know Day. The theme in 2022 was *Artificial Intelligence, e-Governance and access to information*. The focus on enabling digital access built upon the release last year of the *Open by Design Principles*, which outline important considerations for government agencies to build a culture of transparency and trust by prioritising, promoting and resourcing proactive disclosure.

National and international cooperation

Association of Information Access Commissioners (AIAC)

The Information Commissioner, together with other commissioners and ombudsmen in Australia and New Zealand, is a member of the AIAC. All members have a complaint and review jurisdiction over access to information legislation. Meetings are held twice a year to collaborate and discuss common issues and share knowledge and resources between jurisdictions.

Privacy Authorities of Australia (PAA)

The Information Commissioner is a member of a group that is comprised of commissioners and ombudsmen with jurisdiction over privacy laws in Australia. Meetings are held twice a year. OIC staff members also participated in a number of PAA forums to discuss topical privacy issues with policy officers from other jurisdictions.

Asia Pacific Privacy Authorities (APPA)

The OIC is a member of APPA, a forum for privacy authorities in the Asia Pacific region. It gives privacy authorities in the region an opportunity to form partnerships, discuss best practices and share information on emerging technology, trends and changes to privacy regulation.

[11] https://infocomm.nt.gov.au/abou.t-us/news/articles/privacy-awareness-week-1-7-may-2023.

Appendix 1 - OIC Financials

Detailed financial information regarding OIC operations now appears in the Ombudsman's Annual Report (in particular see the '*Comprehensive operating statement by output group*' at note 3 to the Financial Statements).

Figures have been rounded to the nearest thousand dollars, with amounts of $500 or less being rounded down to zero. Figures may not equate due to rounding.

OFFICE OF THE INFORMATION COMMISSIONER EXPENSES

For the year ended 30 June 2023

	2022-23
EXPENSES	**$000**
Employee expenses	395
Administrative expenses	40
Purchases of goods and services	*37*
Accommodation	2
Communications	2
Information Technology Charges	10
Insurance Premiums	-
Legal Expenses	11
Marketing & Promotion	2
Memberships and Subscriptions	1
Motor Vehicle Expenses	6
Official Duty Fares	-
Other Equipment Expenses	-
Training and Study Expenses	3
Travelling Allowance	1
Property management	*3*
TOTAL EXPENSES	**435**

NOTE: Some categories of expenses are incurred by the Business Services Unit on behalf of all Ombudsman's Office work units. These include records storage, consumables/general expenses and stationery. They do not appear above.

Appendix 2 - Statistics by Organisation

The following public sector organisations received or handled FOI applications during 2022/23. We appreciate their co-operation and assistance in the timely and accurate reporting of the information necessary for this report.

The abbreviations reflect titles and responsibilities at 30 June 2023.

Abbreviations for public sector organisations

AAPA	Aboriginal Areas Protection Authority
AGD	Dept. of the Attorney-General and Justice
BGCG	Belyuen Community Government Council
CDU	Charles Darwin University
CMC	Dept. of the Chief Minister and Cabinet
CoD	City of Darwin
CoP	City of Palmerston
DCDD	Dept. of Corporate and Digital Development
DEPWS	Dept. of Environment, Parks and Water Security
DIPL	Dept. of Infrastructure, Planning and Logistics
DITT	Dept. of Industry, Tourism and Trade
DoE	Dept. of Education
DoH	Dept. of Health
DTF	Dept. of Treasury & Finance
EARC	East Arnhem Regional Council
LRC	Litchfield Regional Council
LSNT	Law Society
OCM	Office of the Chief Minister
OCPE	Office of the Commissioner for Public Employment
PFES	Police, Fire and Emergency Services
PWC	Power and Water Corporation
TFHC	Dept. of Territory Families, Housing and Communities
TIO	Territory Insurance Office

TABLE 1 – Access applications and outcomes 2022/23

Details as advised by Organisations.

Org	Total Lodged	Full release	Part release	All exempt	Finalised other basis#	Total Finalised*
AAPA	2	2	0	0	0	2
AGD	194	15	112	10	84	221
BCGC	1	0	0	0	1	1
CDU	12	12	0	0	1	13
CMC	21	3	9	3	6	21
CoD	8	7	0	0	1	8
CoP	5	2	1	0	2	5
DCDD	15	2	3	0	4	9
DEWPS	31	3	11	3	10	27
DIPL	65	17	11	6	28	62
DITT	36	6	11	1	22	40
DoE	62	9	28	0	21	58
DoH	439	221	67	0	161	449
DTF	4	0	1	0	2	3
EARC	1	0	0	0	1	1
LRC	2	1	0	0	1	2
LSNT	1	1	0	0	0	1
OCM	20	3	5	2	16	26
OCPE	4	0	2	0	1	3
PFES	298	28	158	46	96	328
PWC	2	0	0	0	2	2
TFHC	441	24	281	13	75	393
TIO	6	6	0	0	0	6
TOTAL	**1670**	**362**	**700**	**84**	**535**	**1681**

Notes:

For more detail on applications with other outcomes, see Table 1A.

* Outcomes may include matters carried over from the previous period.

TABLE 1A – Access applications finalised on another basis 2022/23

Details as advised by Organisations.

Org	Withdr	Transf	s18	s27	Fees	Excl	s25	Other	Total
AGD	3	2	8	9	1	1	24	36	84
BCGC	0	0	0	0	0	0	0	1	1
CDU	0	0	0	0	0	1	0	0	1
CMC	2	3	0	1	0	0	0	0	6
CoD	0	0	0	1	0	0	0	0	1
CoP	1	1	0	0	0	0	0	0	2
DCDD	2	1	0	1	0	0	0	0	4
DEWPS	3	1	3	3	0	0	0	0	10
DIPL	8	1	9	5	3	0	1	1	28
DITT	12	4	2	1	0	0	3	0	22
DoE	4	0	1	16	0	0	0	0	21
DoH	36	0	99	20	6	0	0	0	161
DTF	2	0	0	0	0	0	0	0	2
EARC	0	0	0	0	1	0	0	0	1
LRC	0	0	0	0	1	0	0	0	1
LSNT	1	6	1	7	1	0	0	0	16
OCM	0	1	0	0	0	0	0	0	1
OCPE	36	2	11	18	3	15	0	11	96
PFES	0	0	0	0	0	0	0	2	2
TFHC	18	6	3	48	0	0	0	0	75
TOTAL	**128**	**28**	**137**	**130**	**16**	**17**	**28**	**51**	**535**

Notes:

Wthdr	Withdrawn
Transf	Transferred
s18	Invalid application
s27	Information does not exist, could not be identified or located
Fees	Non-payment of fee or deposit
Excl	Excluded from application of the Act or not covered by Act
s25	Unreasonable interference with operations
Other	Any other reason

TABLE 2 – Information correction applications and outcomes 2022/23

Details as advised by Organisations.

	Lodged	As Requested	Other Form	No Change	Withdrwn	Finalised
AGD	1	0	0	1	0	1
DoH	4	1	0	0	5	6
PFES	2	0	0	2	0	2
TOTAL	**7**	**1**	**0**	**3**	**5**	**9**

Note: In addition a small number of applications were carried over from 2021/22.

TABLE 3 – Internal Review applications and outcomes 2022/23

Details as advised by Organisations.

	Lodged	s103(2)	Confirmed	Varied/ Revoked	Wdrn	s39A	Finalised
AGD	5	0	5	0	0	0	5
CMC	2	0	1	1	0	0	2
CoD	1	1	1	0	0	0	1
DCDD	1	0	1	0	0	0	1
DEPWS	2	0	2	0	0	0	2
DIPL	5	0	2	2	0	0	4
DITT	5	1	3	3	0	0	6
DoE	1	0	0	1	0	0	1
DoH	1	0	0	2	0	0	2
OCM	1	0	1	1	1	0	3
PFES	12	1	8	1	0	0	9
TFHC	4	0	4	0	0	0	4
TOTAL	**40**	**3**	**28**	**11**	**1**	**0**	**40**

Note: In addition a small number of applications were carried over from 2021/22.

TABLE 4 – Application Fees 2022/23

Details as advised by Organisations.

Organisation	Fees Received	Reduced/ Waived	Reduction
AAPA	60	0	0
AGD	690	6	180
CDU	30	0	0
CMC	540	0	0
CoD	180	2	60
CoP	150	0	0
DCDD	240	0	0
DEPWS	750	0	0
DIPL	1200	2	60
DITT	810	2	60
DoE	150	0	0
DoH	1020	21	630
DTF	60	0	0
LRC	30	0	0
LSNT	0	1	30
OCM	390	1	30
OCPE	60	0	0
PFES	2820	5	150
TFHC	570	4	120
TOTAL	**$9,750.00**	**44**	**$1,320.00**

TABLE 5 – Processing Fees 2022/23

Details as advised by Organisations.

Organisation	Fees Received	Reduced/ Waived	Reduction
AGD	8331	0	0
CMC	2187.43	9	1050
CoP	50	0	0
DCDD	1145.28	1	100
DEPWS	7853.99	5	324.75
DIPL	1353.75	4	421.14
DITT	4058.24	3	1096.02
DoE	443	0	0
DoH	2385.2	27	1827
DTF	325	0	0
LRC	325	0	0
OCM	380	13	1527.5
PFES	7299	0	0
TFHC	2663.35	7	977.27
TOTAL	**$38,800.24**	**69**	**$7,323.68**

Office of the
Information Commissioner

GPO Box 1344 Darwin NT 0801

Freecall 1800 005 610

infocomm@nt.gov.au

http://www.infocomm.nt.gov.au

NT House, 22 Mitchell Street

Darwin NT 0800