Responding to requests and complaints well

Overview

Organisations need to have robust processes in place for responding to access and correction requests. They also need complaint mechanisms with clear escalation pathways that enable them to support individuals who feel they have had their privacy rights affected. Complaints can often be resolved by an organisation directly, with a clear process and supporting guidance.

The way that an organisation responds to access and correction requests and complaints can build or undermine the trust and confidence that clients, customers and employees have in the organisation.

This pou provides guidance on:

- Responding to access and correction requests.
- Complaints handling.

Who is this for?

Your organisation's privacy function, as well as those who:

- Receive and escalate access and correction requests, privacy complaints, and enquiries.
- Action and respond to access and correction requests, privacy complaints, and enquiries.

Key objectives of the Responding to requests and complaints well pou

What would we expect to see?

- Complaints and access and correction request information is easily accessible to individuals.
- Organisation has clear escalation pathways for complaints and established processes for managing individual requests.

Access and corrections requests

Individuals have access and corrections rights and organisations have legal obligations to respond promptly to requests for access and correction. If you don't meet these obligations, individuals have the right to complain to OPC. If OPC investigates the complaint, the individual has the right to take their complaint to the Human Rights Review Tribunal.

How do I deal with an individual's request for their personal information?

You need to provide individuals with access to the personal information you hold about them, if they ask for it, subject to a very limited number of exceptions. There are some steps you'll

need to work through if you receive a request for personal information, even if the requester doesn't mention the Privacy Act:

1. Work out whether you hold the personal information that the person has asked for. If you don't, but you know another organisation holds the information, you should consider whether it would be appropriate to transfer the request to that organisation. Otherwise, you will need to refuse the request. You should also verify the identity of the requester to ensure they are the subject of the personal information being requested, or an authorised representative.
2. Once you've established that you hold the information, the next thing to decide is whether you're the right organisation to release it. If you know the information is also held by another organisation, and you think it would be more appropriate for that organisation to decide whether to provide the information, then you should transfer the request to that organisation. If you transfer the request, you need to do so within 10 days of receiving it. However, you shouldn't transfer a request if you know the individual wouldn't want you to.
3. If you hold the information, and haven't transferred the request to another organisation, then you'll need to decide on the request. Generally, this must be done within 20 working days. However, the timeframe could be shorter if the individual has grounds to ask for the information urgently, or it could be longer if you have grounds to seek an extension. If you extend the timeframe for responding, you must inform the individual of the extension within the 20 working days and let them know they can complain to OPC about the extension. Equally, if the request is straightforward and doesn't require your organisation to gather much information, then it should be addressed quickly.
4. When you do provide a decision, it must say whether you agree to release all of the information requested, some of the information, or none of the information. If you aren't releasing all the information, you need to provide a reason why, and tell the individual of their right to complain to OPC.

Additional obligations:

- Instead of refusing a request for personal information, you could consider imposing conditions. For example, you might want to restrict how the requestor can use the information. However, you need to be able to explain why any limit or condition is necessary.
- You must make the information available in a way preferred by the requestor, unless the exceptions in s56(2) of the Privacy Act apply.
- You need to consider your organisation's responsibilities in s57 of the Privacy Act before giving access to the information.

Do I respond under the Privacy Act or the Official Information Act?

Responding under IPP6 – someone asking any organisation for information about themselves

If an individual asks for their own information, the Privacy Act will apply, regardless of whether that information is held by a public or private sector organisation.

If an individual uses a representative, or someone who has Power of Attorney or Enduring Power of Attorney for them, then that representative is acting on the individual's behalf. A family member can also request an individual's information on their behalf, if they have their

written authority to do so – this can be done via letter or email. Your organisation will need to respond as if that individual is asking for their information directly.

It's also important to note that the Privacy Act doesn't provide parents or guardians with a general right to request their child's personal information. However, if the child is either too young to act on their own behalf, or if they have given authorisation, a parent or guardian can request information.

Responding under IPP11 – someone asking private sector organisations for information about other people

If someone asks a private sector organisation for information about another individual, the Privacy Act also applies. Before disclosing information about another individual, the organisation will need to consider whether privacy principle 11 allows it to disclose the information. While organisations may disclose personal information where an exception under principle 11 applies, this is completely discretionary. In other words, an organisation doesn't have to disclose someone else's personal information to someone else if it doesn't want to, regardless of whether it could rely on an exception under principle 11.

If the information is held by a public sector organisation, the Official Information Act (OIA) may apply, or the Local Government Official Information and Meetings Act (LGOIMA) for local government bodies.

Responding under the OIA/LGOIMA – someone asking a public sector organisation for information about other people

If someone asks a public sector organisation for information that is solely about another individual (not the requestor), a company, or other types of information – such as business information or copies of policies – then the OIA will apply, or the LGOIMA for local government bodies.

Any privacy issues need to be considered under the provisions of those Acts that allow information to be withheld on privacy grounds. Privacy is a good reason for declining an official information request unless there's strong enough public interest to outweigh the privacy concerns.

Responding where the information is about the requestor and another person

If someone asks for information that is both about themselves *and* about another person, the Privacy Act will apply. This is commonly called 'mixed information'.

Clarifying scope with the requestor

Section 42 of the Privacy Act requires an organisation to give reasonable assistance to a requestor. This includes helping them to make the request, or making sure that the request has been made to the right organisation. It can also enable an organisation to ask the requestor to focus their request if it's too broad.

A simple way to focus the request is to ask the requestor to complete a personal information request form, if your organisation has one. But you can't demand that they do this. Using a templated form encourages requestors to be as specific as possible when describing what personal information they seek.

If this doesn't reduce the scope of the request, an organisation can ask the requestor some questions to further understand it:

- What is the purpose of your request? (note that you cannot demand this information or consider it when deciding whether to release information).
- Are there any kinds of information you're looking for, or places you believe it might be held?
- Why do you believe the organisation might hold this information about you?
- Is there a particular timeframe your request relates to?
- Are there particular events you are aware of that relate to you?
- Which staff have you previously dealt with at the organisation?

Charging for access to personal information

In most circumstances, you shouldn't charge people to access or correct their personal information. However, there are some circumstances where it might be appropriate for an organisation to charge, and there are special rules that apply to health or credit organisations.

For more information see our guidance on charging for access to personal information.

Refusing access to personal information

If someone asks for access to the personal information your organisation holds about them, you must give it to them unless there is a reason to withhold it under the Privacy Act.

You may be able to withhold information if:

- It isn't readily retrievable.
- Releasing it could negatively affect the requestor's mental health.
- Releasing it could put someone else in danger.
- Releasing it would breach someone else's privacy.
- It was provided in confidence.
- You don't have it.
- The request is trivial.
- The request is vexatious.

The above list is not exhaustive. For more information on these refusal reasons, use the quick links below:

What does readily retrievable mean?
Can I withhold information to protect someone's mental health?
Can I withhold information to protect someone's life, health, or safety?
When can I refuse a request for mixed personal information?
Can I withhold information provided in confidence?
What if we don't have the information someone has requested?
What makes a request trivial?
What makes a request vexatious?

How do I respond to a request to correct or delete information?

Individuals have a right to request the correction of any personal information you hold about them, including asking for their information to be corrected by removing or deleting it. If you decline to correct the information as requested, then the individual has the right to ask to have a statement of correction added to the information in question.

Once you receive a request for correction and/or a statement of correction, you have 20 working days to review the information in question and decide whether to make the correction requested.

You don't necessarily have to make the correction if you consider that the information is already accurate, or there might be good reason why you can't change a historic record. However, you should also keep in mind that you have an obligation to make sure personal information is accurate before using it and, as such, there could be issues leaving inaccurate or disputed information on someone's file.

Once you have decided how you will respond to the request for correction, you should let the individual know if you will be making the correction or not. If not, you should let them know they have the right to provide you with a statement of correction if they haven't done so already. The statement of correction needs to be kept attached to the information they asked to be updated, in a way that they will always be read together.

You should also let the individual know that they have the right to review your decision not to correct the information, by making a complaint to OPC.

When you have made a correction, or attached a statement of correction to personal information, you must also, so far as is reasonably practicable, inform every other person your organisation has disclosed the information to.

Complaints handling

Having a robust process to respond to complaints, with clear pathways for escalation, will help your organisation support individuals who have privacy concerns. Complaints can often be resolved by an organisation directly, with a clear process and supporting policies. Individuals need to try and work with organisations to resolve their complaint before complaining to the Privacy Commissioner.

OPC will often refer a complainant back to the organisation to try and resolve a complaint in the first instance.

Some key considerations include:

- It should be easy to make a complaint. For example, does your organisation have information on its website about how to make a complaint, and is it easy to find and understand? You could also consider having a feedback or complaint form available in both print and electronic formats.
- How are privacy complaints identified and escalated to the right people? There should be clear processes and policies in place to ensure privacy complaints are dealt with by staff with good understanding of the Privacy Act.
- Regularly review your complaints data to spot trends or issues. If there are repeated issues being raised by complainants, that's important information you can use to uplift your privacy practices.
- Proactive notification of breaches. It's a requirement to notify serious harm breaches; being well prepared to notify OPC and affected individuals of a privacy breach can help avoid potential complaints. This should be part of your organisation's breach management and incident response plan. For more information see our Breach Management guidance.

Communicating with a complainant

It's important to acknowledge a complaint promptly and inform the complainant of what the next steps are.

Your initial response should generally cover the following points:

- Acknowledgement of the complaint.
- Your understanding of the issue.
- Who will be looking into the complaint.
- What the complainant expects as an outcome, if they haven't included this.
- When you will be in contact with the complainant again.

Investigating the complaint

You should consider the following matters, when investigating the complaint:

- What happened?
- Which privacy obligations and/or principles are relevant and why?
- Has your organisation complied with its privacy obligations?
- Were internal process and policies followed? If not, why weren't they?
- Can you take any steps to resolve the complainant's concerns?
- Has the investigation into the complaint identified a notifiable privacy breach?

Sometimes organisations will seek an independent review into a privacy complaint or breach. These reviews often provide the organisation with recommendations and can be a useful way to support transparency and get independent feedback for improvement.

Providing a response

Your response to the complainant should be written in plain language and include:

- The information you have relied on when developing the response, and the outcome of your investigation into the complaint.
    - Make sure you've considered the appropriateness of providing all the information that was relied on. For example, where personal information is being withheld because providing it would prejudice the interest being protected.
- An invitation for the complainant to reply to your response, or an offer to meet or discuss further if appropriate.
- An apology if you did not comply with the privacy obligations in question, and details of any additional outcomes that you have considered. For example, a change in procedure, amending your policy, or providing additional privacy training to staff.
- Information about the complainant's right to complain to the Office of the Privacy Commissioner if they are not satisfied with the outcome.
- Whether you have notified OPC (if the complaint identified a notifiable privacy breach).

OPC's process

There is information about our investigations and dispute resolution process on our website, along with our Decision Guide. OPC is proud of the work we do in the area of dispute

resolution. Where it is appropriate, we try and bring the parties together, in person or by phone, to resolve privacy disputes.

Many of the resolutions we help to facilitate include an apology or an acknowledgement, and may include a promise of confidentiality, a change in an organisation's processes, staff retraining, or a compensatory payment.

Where we are unable to assist the parties to resolve the dispute, we can:

- Decide not to investigate, for example, if we are of the view that there is an alternate dispute resolution process that it would be reasonable for the complainant to pursue.
- Initiate or continue with an investigation, with a view to reaching a final view on whether the complaint has substance (i.e. has there been a breach of the Privacy Act and has this caused some kind of harm which requires resolution?); or
- Where the complaint concerns access to personal information, make an access direction.

OPC cannot award damages, and the payment of compensation or costs during our processes can only occur by agreement of the parties. However, if a settlement is not reached, the aggrieved party can initiate proceedings in the Human Rights Review Tribunal (the Tribunal). The Tribunal can compel parties to take certain actions and can award damages, as well ordering the payment of costs. The Tribunal can also hear appeals by organisations against access directions made by the Commissioner.

Many New Zealanders have learned the hard way of the time, cost and emotional drain of litigation, and the delays inherent in the Tribunal process. While proceedings in the Tribunal are intended to be inexpensive and accessible, they inevitably involve costs for both parties; be it time, financial or emotional costs, or a combination thereof.

Apologies

It makes good sense for both parties to engage in settlement discussions early, and to make genuine attempts to resolve the matter. Ideally, this will result in an agreed settlement that both parties can live with, avoiding the need for us to continue with our investigation, or for parties to go to the Tribunal at all. However, as the following examples illustrate, a party's genuine attempt to settle the matter can also be effective in reducing their financial liability if, despite their best efforts, the matter still proceeds to hearing.

Very often, we find that complainants who have a sense of hurt and anger due to the actions of an organisation, simply want that hurt recognised, and for an apology to be issued.

To be most effective, apologies must be sincere and should be offered early. We continue to see apologies that fail to convince a complainant, as well as organisations that are reticent about apologising for fear that if a settlement is not reached it will be used against them in later proceedings.

The following points are worth noting:

- Ideally, an apology should acknowledge the hurt caused by the organisation's actions/inactions, apologise and, if appropriate, briefly explain the steps the organisation has taken to prevent the issue from occurring again.
- An appropriate and timely apology can be considered by the Tribunal when considering whether the defendant's conduct has addressed the harm suffered by the complainant because of the breach of privacy. There are a number of case

examples where an effective apology has been assessed by the Tribunal and resulted in a lower damages award that would have otherwise been the case (see for example Williams v ACC [2017] NZHRRT 26 and Marshall v IDEA Services Ltd [2020] NZHRRT 13).

- In contrast, apologies made too late in the process will not help the complainant and may have no "measurable consequence in the context of the assessment of remedies" (Vivash v ACC [2020] NZHRRT 16).
- The Privacy Act now expressly protects apologies from being used as evidence against an organisation in any civil proceedings brought under the Act. The inclusion of section 100 in the 2020 Act is intended to support organisations to offer prompt, genuine and sincere apologies without concern as to how this may impact on their legal position if the complaint cannot be resolved between the parties. The ability for the Tribunal to take account of an apology when assessing of remedies to be awarded against the organisation has been expressly retained.

Should you make a settlement offer?

Litigation is expensive. While you can act for yourself, the way that you conduct your case could expose you to having to pay legal costs, or increased costs, to the other side. Refusing to accept a reasonable settlement offer could be relevant to whether you could be ordered to pay costs if you are not successful in the Tribunal. This blog focuses on settlement offers, however, other factors, such as acting in bad faith, will also be relevant to the Tribunal's decision on costs.

The usual rule of thumb is that "costs follow the result" – in other words, the losing party must pay 'costs' to the other side, with the amount being determined by the Tribunal (if the parties fail to agree). The Tribunal has considerable discretion when awarding costs, and its unique human rights jurisdiction means that it may depart from the conventional rules applying to civil proceedings where that is necessary to do justice in particular case.

In most cases successful claimants will be entitled to an order of costs. However, it is important that claimants are aware that this will rarely (if ever) reflect actual costs incurred (and if you are representing yourself, it is also important to note that costs are awarded to reflect the money that you have spent during the proceedings. If you have not engaged legal counsel, you may be able to obtain costs for your disbursements, but not for the time that you've spent on the case). Defending proceedings in the Tribunal can also be very costly for organisations. Even if the action is unsuccessful, costs awards to organisations, if made at all, are usually only a small fraction of the actual money spent by the organisation defending the proceedings.

It therefore makes sense for both parties to engage in settlement discussions early in this process, and to make genuine attempts to resolve the matter. You can do this "off the record" by marking your written correspondence as being "without prejudice" or using this language in your discussions. This means that this information cannot be admitted in evidence in court proceedings and cannot prejudice your legal position in the Tribunal.

You can also make a settlement offer on a "without prejudice except as to costs basis". This means that the correspondence cannot be put before the Tribunal when it is deciding whether there has been an interference in privacy but can be put before the Tribunal when making a decision on costs (these are often called Calderbank offers).

Offers made on this basis can be a very useful tool to progress reasonable and early settlement of proceedings as they encourage parties to realistically appraise their position in litigation.

In particular:

- If a reasonable offer of settlement is rejected, a claimant may find that no costs are awarded, or they are required to pay some, or all, of the other side's costs (see for example, Turner v University of Otago [2021] NZHRRT 48); and
- A respondent's failure to accept a complainant's reasonable settlement offer can also be relied on by the Tribunal to justify a higher costs award than would otherwise be the case.

Our repeated reference to "reasonable" is deliberate. Like with apologies, a bad offer can further inflame the situation and potentially backfire on the party that offered it. Whether a Calderbank offer is "reasonable", and therefore whether it is reasonable for a party to have rejected a Calderbank offer, must be assessed at the time at which the offer is made and declined. In Cook v Manawatu Community Law Centre [2021] NZHRRT 57, for example, the Tribunal held that although the respondent made a Calderbank offer which was greater than the final awarded amount, the applicant was still entitled to reject the offer at the time given her desire for vindication and finding the truth.

While there is no easy formula for 'valuing' a complaint, the Tribunal's decision in Hammond v Credit Union Baywide [2015] NZHRRT 6 provides useful guidance, grouping damages for emotional harm into three broad bands: *"At the less serious end of the scale awards have ranged upwards to $10,000. For more serious cases awards have ranged between $10,000 to about (say) $50,000. For the most serious category of cases, it is contemplated awards will be more than $50,000".*

A table of recent Tribunal awards is also available online.

We have also provided an overview of some of the recent settlements that we have facilitated, which may assist parties in their formulation or consideration of settlement offers, in our post detailing how OPC works to settle complaints.

Organisation examples

We've included some use cases based on fictional organisations to demonstrate each of the pou in practice. Read more about them in Introducing the Organisation Examples.

Large business – Fern Leaf

Fern Leaf typically handles complaints from its customers. There is a dedicated Customer Resolutions Team who work closely with the privacy team to identify complaints where there might have a privacy impact. The Customer Resolutions team has received training on spotting personal information requests and possible breaches that need investigating. Fern Leaf has clear guidance on its websites about how individuals can make a complaint to them.

The Privacy team in turn tracks and monitors the number of complaints with a privacy angle, as well as number of access or correction requests. While it is not a right under the Act, Fern Leaf have decided it is good privacy management to also track the number of deletion requests. All monitoring includes looking at timeframes.

Small business (charity) – Reach High

When it comes to access requests and complaints, as a small organisation Reach High has decided to implement a centralised privacy operating model. This means that all access requests and privacy complaints are escalated to the Director of Support Services, who logs them in the Privacy Risk Register and manages them with the help of other managers where required.

Start-up – Swiftstart NZ

As Swiftstart NZ holds personal information on behalf of its clients, it doesn't get many access or correction requests. In the rare case they do, they seek advice internally from their operations manager (who is responsible for any legal and compliance issues) about whether to transfer the request to the organisation that they're providing the service on behalf of. Swiftstart NZ also have their own internal processes for managing requests and complaints about the client personal information they do manage (account holder contact information etc.), and these are logged in a Privacy Requests and Complaints register.

Small business (non-tech) – Green Gardens

As the Privacy Officer for Green Gardens, the Administrator manages any access or correction requests, and complaints. These are logged in a Privacy Requests and Complaints register and escalated to the Owner/Manager if required.

Independent contractor – Jo Jones

Jo Jones manages any access and correction requests and complaints from her clients. These are logged in a Privacy Requests and Complaints register. When working with a community health service provider, Jo Jones doesn't receive or deal with the access and correction requests and complaints, these are managed by the privacy function within that organisation. However, whenever a request or complaint is received from one of her clients, she works with the privacy function as necessary to fulfil the request or resolve the complaint.

Government agency – The Ministry

Customer service staff respond to most access and correction requests, in line with guidance that is developed by the Privacy team, and with the ability to escalate to the privacy team if needed. Complaints come in directly to the Privacy team. The Ministry doesn't get huge numbers of requests or complaints, but it does routinely review the ones it does get to see if there are ways that the Ministry can improve how it responds to access and correction requests, and privacy complaints. There is reporting from the customer service team into the privacy team about the numbers of requests received and the timeliness of responses, which is then aggregated and reported up to SLT quarterly.