PRIVACY AT NETSAFE

Netsafe is New Zealand's independent, non-profit online safety organisation. Many of the services we deliver, including under the Harmful Digital Communications Act (HDCA), require us to collect and use personal information – information about people.

This privacy statement explains what personal information we collect, how we store, use and share it, and how you can access or correct your own information.

Our values of accountability, transparency and inclusiveness align with good privacy practice. Netsafe's board and team understand their privacy obligations and are accountable for the information we hold. This privacy statement is our way of ensuring openness and transparency about our privacy practices and helping the people we deal with have some control over their information.

Here are a few important things to know:

- We only collect (or generate) the personal information we really need to carry out our functions and deliver services
- We take great care to balance individual privacy against our obligations to deliver services and meet our legal obligations, and we will only share personal information where we consider it is necessary or you have authorised it
- We store personal information in the cloud with our trusted service providers, Zendesk and Microsoft Azure, and we use Microsoft Office 365 applications. We protect our data with all reasonable technical, contractual and process controls
- You can ask us for a copy of your personal information at any time. We will be as open as we can with you, but we must balance your right to know against the privacy and safety of others

If you can't find the information you need below, or you have concerns about the way we are managing your personal information, then please contact our Privacy Officer any time at help@netsafe.org.nz.

We may update this privacy statement from time to time, for example to reflect changes to the Privacy Act, so take another look occasionally to see what might have changed. This statement was last updated in November 2020.

How we collect personal information

We only collect (or generate) the personal information we really need to carry out our functions and deliver services.

Some of the services we deliver do not require you to give us personal information. For example, you can report a scam or other online issue anonymously. However, if you need us to assist you in some way, or if you want to make a report under the HDCA, we will need to know who you are, and collect some of information about your circumstances.

We collect personal information directly from you when you engage with us. We may also collect personal information about you from third parties, for example if you are party to a complaint or a report under the HDCA. We also generate personal information as we carry out our functions.

Personal information we collect to deliver online safety services

Our HDCA and online safety functions require us to collect more personal information than any of our other functions. We may collect personal information about a person asking for assistance with a scam or reporting harmful digital content (a reporter), a victim of harmful digital content (a target), or a person alleged to have posted harmful content (an alleged producer). Whatever the context, we only collect what we really need.

The personal information we may collect or generate as part of delivering services includes:

- name
- contact details, including your address, email address or phone number
- the region you're located in
- age group
- gender
- ethnicity
- online usernames
- date and time of your report
- details of your report
- evidence of harmful content or online abuse, including screenshots and documents
- evidence of harm caused by harmful content or online abuse, which may include health information
- external complaint correspondence, including with the parties to a complaint or with other agencies like platform providers
- internal complaint correspondence, such as communications with managers to ensure we are managing a complaint appropriately
- our assessments of a complaint or report
- file notes of calls or meetings
- call recordings
- any other information you choose to provide to us

We may also collect publicly available information about you – such as media reports or public social media content – where this is relevant to carrying out our functions or delivering services.

Personal information we collect to manage public engagement

We may also need to collect and use a small amount of personal information to effectively engage with other agencies and the public about the work we do. However, we only collect the personal information you choose to give us, and you can opt out of our communications activities, such as receiving our newsletter, at any time. Our engagement activities include managing requests for resources, presentations or subscriptions to our newsletters, running surveys or research and ensuring our website is effective.

The information we may collect when you engage with us includes:

- your name (if you choose to provide it)
- your contact details, including your address, email address or phone number
- details of any services you request, including resources, presentations or subscriptions
- your subscription status (parent, educator or online safety professional)
- your responses to surveys or focus group discussions (usually these will be captured in a de-identified form)
- information about your use of our website (explained further below)

We collect the following information about your use of our website (though please note we make no efforts to associate this with your identity):

- your IP address
- the search terms you used
- the pages you accessed on our website and the links you clicked on
- the date and time you visited the site
- the referring site (if any) through which you clicked to our website
- the device you used to access the site
- your operating system (for example, Windows XP, Mac OSX)
- the type of web browser you use (for example, Google Chrome, Internet Explorer or Mozilla Firefox)
- incidental information (for example, screen resolution, Flash version, or language setting of your browser)

We use cookies to generate a lot of the information listed above, including to track the way you have used our website. Cookies are small text files that are sent by a website and stored on your computer's hard drive. You can manually disable cookies at any time in your browser settings, however, there may be some services on the site that do not work when cookies are disabled (such as the report pages for reporting content) .

How we use and share personal information

We take great care to balance the privacy rights of all the people we deal with against our need to effectively carry out our functions, meet our legal obligations and keep people safe. This means that we may need to share personal information about you, but we will only ever do so when we believe it is necessary.

We use personal information to meet our lawful purposes

In order to carry out our functions and deliver services, we need to use your personal information in the ways set out below. Where we need to use information in a way we have not anticipated here, we will only do so if required or permitted by law or with your authorisation.

We will use your personal information to:

- respond to and investigate incident reports, enquiries or other requests for assistance
- assess incidents, including deciding whether they breach the communications principles or have caused harm

- resolve complaints about harmful digital content in accordance with the requirements of the HDCA
- manage safety risks to people we deal with
- assist our national partners, including law enforcement and other government agencies, to manage risk and investigate or prosecute criminal offences relating to harmful digital content, online abuse or fraud
- meet the reporting requirements of our funding partners
- identify and analyse report, complaint or enquiry trends
- review and improve the delivery of our services, including auditing quality and performance
- train our staff
- educate others about online safety and compliance with the HDCA
- communicate with you about online safety topics via our newsletters and email updates
- (with respect to website data only) analyse website usage and improve website functionality and experience

We share personal information only when we must

To meet the uses and purposes set out above, and to effectively carry out our functions and meet our legal obligations, we may need to share your personal information with other people or agencies. We will always try to let you know before we share your information and, where we can, we will ask for your authorisation. But we may also need to share information without your authorisation (for example, where we believe you are at risk) or if it is in accordance with the law.

Where we believe it is necessary to share your personal information with a third party, we will only ever share the minimum amount required to meet our purposes. For example, we may only need to share a summary of your report or complaint, not the documentation or evidence you have provided to support it.

We may need to share your personal information with:

- the other party to a complaint or report, for the purposes of resolving it or if that person makes a Privacy Act request for their own information (we always consider the privacy interests of both parties when managing this)
- one of our national partners, where we believe they may be able to assist with or take over the management of an incident or resolution of a complaint or report, including:
    - Privacy Commissioner
    - NZ Police and OCEANZ
    - Commerce Commission
    - Department of Internal Affairs
    - Financial Markets Authority
    - Ministry of Consumer Affairs
    - CERT NZ
    - NZ Customs Service
- certain people, law enforcement or government agencies, where we believe that you are at risk of harm, including:
    - NZ Police and OCEANZ
    - Oranga Tamariki
    - your school

    - your parents or whānau
- the online platform that is hosting harmful digital content, where we are assisting you to have the content removed (for example, Facebook, Twitter or Google)
- the District Court, where required for the purposes of facilitating legal proceedings under the HDCA
- our funding partners – Ministry of Justice and Ministry of Education – to meet our reporting requirements (though this will usually be aggregated and anonymised data)
- a person who has requested information under the Official Information Act that includes personal information about you, though we will withhold personal information from an OIA response if we can

We share personal information with third party providers for marketing purposes

We use Mailchimp for sending our emails and as our marketing automation platform. As such, we share some of your personal information with Mailchimp in order to send you newsletters and updates about relevant topics of interest. By joining our mailing list, you acknowledge and authorise that the information you provide will be transferred to Mailchimp for processing in accordance with its Privacy Policy.

For information on how to opt out of Mailchimp data analytics, visit the Mailchimp preferences page.

How we store and protect personal information

We store personal information in the cloud with our trusted service providers, Zendesk and Microsoft Azure, and we use Microsoft Office 365 applications. We protect our data with all reasonable technical, contractual and process controls.

Storage and retention

We use trusted third-party providers to store and process our data, because we believe this is more secure and cost effective. We store most of the personal information we collect and generate on two cloud-based platforms:

- Information about our incident reports and HDCA complaints, including person details, correspondence, assessments and file notes, is processed and stored within Zendesk.
- We store and process some information on Microsoft Azure cloud servers, and we use Microsoft Office 365 for our email and other office productivity applications.

This means that the personal information we hold may be transferred to, or accessed from, countries other than New Zealand. To better protect our data, we have restricted its location at rest. Our data in Microsoft Azure is located in Australia. Our data in Zendesk is located in the US.

We have contracts in place with both Zendesk and Microsoft that ensure we maintain control over our data, including documents, stored or processed on our behalf.

We retain personal information only for as long as we need it. In general, we destroy personal information two years after the last action we have taken on the matter to which it relates. However, we delete any recorded phone calls after three months (unless it is necessary to keep

them for longer to facilitate legal processes). Where information constitutes a public record, we must retain it for as long as is required by the Public Records Act 2005.

Security

We take all reasonable steps to ensure the personal information we collect is protected against loss, unauthorised access and disclosure or any other misuse. We have a security policy in place help our team protect data. Access to our systems and platforms is controlled and audited.

We also ensure that our cloud-based platforms can meet our privacy and security requirements. You can read about Zendesk's privacy and security practices here, and about Microsoft's privacy and security practices here.

Your privacy rights

You can ask us for a copy of your personal information at any time. We will be as open as we can with you, but we must balance your right to know against the privacy and safety of others

The Privacy Act gives you rights to request access to and correction of the personal information we hold about you, whether you've reported an incident, you're a target or you're an alleged producer who has been the subject of an HDCA complaint or report.

You can also take steps to control the ways we use your information (such as opting out of receiving newsletters), and you can complain to us at any time if you think we have misused your personal information.

To exercise any of these rights, please email our Privacy Officer at help@netsafe.org.nz.

Accessing or correcting your information

You have the right to request a copy of the personal information we hold about you (whether we have collected it from you directly or from a third party). You also have the right to ask us to correct your information if you think it's wrong.

We will process your request as soon as possible, and no later than 20 working days after we receive it.

We will be as open as we can with you, but please note that your right to request personal information is subject to the privacy and safety of other people who may be affected by your request. If we believe that releasing information to you might involve the unwarranted disclosure of the affairs of another person, or might increase the risk of harassment or harm to another person, then we may refuse all or part of your request.

If you have made a correction request, and we refuse to correct information because we believe it is accurate, you have the right to attach a statement to the information that explains the correction.

Asking us to stop using your information

You can opt out of receiving our newsletter or being included on any other subscription list by following the unsubscribe link at the end of the email or contacting us. You can opt out of our cookies when you use our website by manually disabling cookies in your website browser.

If you want us to provide you with a service, including resolving your complaint under the HDCA, then we may not be able to stop using your information, especially if we're using it to do something we're required to do by law.

Making a complaint

If you have any concerns about the way we have managed your personal information, or you believe we have unlawfully refused your request for information, please let us know, and we will try our best to resolve it. You can email the Privacy Officer at help@netsafe.org.nz or use our online form.

If we cannot resolve your concerns, then you have the right to complain to the Office of the Privacy Commissioner. Details for making a complaint to the Privacy Commissioner.