IDCARE OFFICIAL POLICY

Identity Care Australia & New Zealand Ltd
(IDCARE)

Privacy Policy

This Privacy Policy covers:

- **What information we collect about you**
- **The circumstances under which we are permitted to share information**
- **How long we retain the information**
- **How you can request that the information be deleted and how you can make a complaint**
- **How you can get help in understanding this policy.**

Date of Endorsement: xx 2024
Version Number: 4.0
Policy Number: xx/2024

Statement of Affirmation

Identity Care Australia & New Zealand Ltd. (ABN 84 164 038 966),IDCARE Limited (4918799) and IDCARE Foundation Ltd (CAN 678 651 986) referred to herein as IDCARE, affirm our commitment to the privacy laws, regulations and principles of Australia and New Zealand.

About this Privacy Policy

This Policy is about your information and the information IDCARE requires about you to perform our services. This Policy informs you about the personal information we collect, retain, use and share with others. It's important that you understand this policy and how you can tell us if you object. If there is anything you do not understand or you would like to have some or all of the policy explained to you, please ask the IDCARE officer you speak to, or email us on help@idcare.org.

Business purpose

Privacy laws mention terms like "business purpose" when it comes to collecting personal information. IDCARE's primary business purpose is providing benevolent services to community members impacted by identity theft, cybercrimes and scams. This includes case management (working with individuals to respond to risks), response and protection services (engaging others on your behalf to reduce risks relating to the misuse of your identity), and informing organisations on how they can improve their response efforts to reduce harm to people in the future. We also connect with the community and educate individuals and organisations about what's occurring, how to prevent this, and how to respond.

The consequences if personal information is not collected:

If all or some of the following personal information is not collected, then IDCARE will not be able to provide you with accurate and relevant assistance.

What we collect, why and how

To enable us to perform our business purpose, IDCARE collects personally identifiable information in the following ways:

Case Management, General Enquiry, Subscriber Enquiry and Get Help Web-Forms

- *Contact information* – your first name, phone number and email address are collected to enable us to get in contact with you, including if the line drops out, and to assist you and to be able to provide you with information relevant to your matter.
- *Basic demographic information* – your postcode, country of residence, gender identity and age range are collected if you agree to provide it, for research and analysis purposes and to help us understand trends and vulnerabilities in scams, identity theft and cyber misuse.
- *Other information* – attributes relating to the exposure or misuse you experienced is collected to enable IDCARE to provide you with relevant information and assistance.

- *Digital device and online information* – attributes such as IP address, device identifier, browser, geo-location approximation, site usage statistics, and online site pathways to IDCARE's Get Help Form, are collected to help us understand whether the crimes people confront are targeting specific devices, applications and locations.

Case Management call recordings

Case management calls to and from IDCARE may be recorded. We tell people when this happens and give them the opportunity to not have the call recorded. If the call recording is turned off, clients will not be disadvantaged in using IDCARE's services. We record calls so that we can help our Case Managers learn and develop. Senior staff and mentors review the content of case management calls, evaluate the planning advice shared, the client reactions and impacts to advice provided, and the adequacy and accuracy of the content.

Website usage

IDCARE's websites (www.idcare.org and www.idcare.org.nz) store cookies on your computer. You may disable these cookies when on those sites. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information to improve and customise your browsing experience and for analytics and metrics about our visitors to our websites and social media platforms.

Some internet search engines also collected limited information relating to access to IDCARE's websites. This includes: Google Analytics (Universal Analytics) with anonymized IP; Google Analytics 4; Google Analytics Advertising Reporting Features; Google Analytics Demographics and Interests reports; Sendgrid. We use this information in order to improve your browsing experience and for analytics and metrics about our visitors to our websites and their interaction with IDCARE web resources.

Technical network and device remediation services and "eDiscovery"

We can provide individuals and organisations with remediation services for devices (eg, mobile phone or computer) and networks that have been impacted by cyber misuse; we call this Cyber First Aid. These remediation services are subject to additional Terms & Conditions, which are also consistent with the provisions of this Policy. To provide these remediation services we may collect further information, including:

- device security settings;
- application security settings (such as email and social media);
- device identification / serial numbers;
- browser security settings and usage;
- anti-virus and anti-malware information.

We also provide a unique service identifier and may provide a Certificate of Completion. These, along with the attributes collected, may be shared with third-parties that have:

(1) requested IDCARE perform these services for the individual or organisation on their behalf (eg, a bank); and/or

(2) would benefit from being informed about new malware, application or related service delivery vulnerabilities.

Identity Verification

If you would like IDCARE to speak to other organisations on your behalf, you will be required to complete an identity verification process. This process requires IDCARE to view your identity, document or related information. We request this information so that we can assure ourselves of your identity in order to act on your behalf. Identity verification data is only obtained with your consent and will include some (not all) of the following types of information:

1. Facial image
2. Full name
3. Date of birth
4. Place of birth
5. Telephone number
6. Residential address
7. Email address
8. Employer's name
9. Driver's licence number, card number, and expiry date
10. Passport number and expiry date (if no Australian or New Zealand Driver Licence)
11. Proof of Age Card (if no Australian or New Zealand Passport or Driver Licence)
12. ImmiCard (if no Australian or New Zealand driver licence)
13. New Zealand Certificate of Identity (if no New Zealand driver licence)
14. Medicare number and Expiry Date.

Verification processes also rely on searching personally identifiable information, including sensitive biometric information, provided to IDCARE by individuals against third party information sources, including identity validation and verification services.

Client Portal

IDCARE manages a Client Portal, directly or via third-party hosted commercial arrangements (such as Microsoft Azure services), which provides a single online identity management system for individuals who opt-in to that system. If you wish to access the Client Portal, you must first undertake an enrolment process as outlined in the Client Portal Terms & Conditions. These consistent with the privacy provisions of this Policy. Users of IDCARE's Client Portal must first agree to these Terms & Conditions.

Any additional protection and response services offered via the Client Portal are subject to separate IDCARE or third party (if delivered by third parties) Terms & Conditions. Where such services rely on responses by third parties, such as Credit Reporting Agencies, law enforcement, financial institutions, and identity credential issuers, individual users will be subject to the third-party Terms & Conditions and Privacy Policy provisions. This will be made clear in the relevant IDCARE Terms & Conditions.

Monitoring and profiling alerts

With your consent, IDCARE may send you alerts in relation to changes detected in your personal information or account usage if detected by IDCARE monitoring, profiling and protection services. The Alerting function requires users to permit IDCARE to send the change notifications to a confirmed mobile phone number and/or email account. The Alerting function within the Client Portal is subject to its own Terms & Conditions, but is also consistent with the provisions of this Policy where privacy matters are concerned.

Collection and use of sensitive information

Except as otherwise outlined in this policy, IDCARE does not generally request sensitive information. However, in providing specialist support services, IDCARE may collect, use and disclose sensitive information (for example, if you share sensitive information with us when using our services). IDCARE will only collect sensitive information where it is reasonably necessary for its functions and activities. We will obtain your consent before collecting sensitive information unless a lawful exemption applies. IDCARE will only use or disclose sensitive information for the purpose for which it was collected, or for a directly related purpose that you would reasonably expect.

Collection and usage of facial imagery

IDCARE captures facial imagery as part of the identity verification process outlined above, if you have provided consent for IDCARE to act on your behalf to contact organisations. Because most identity theft involves the compromise of common identity credential information (such as driver licences and passports), the collection of facial imagery is an important addition to our identity verification process and is matched against third-party templates in a manner that does not involve the retention by that third-party of the templated biometric (ie. the measure of an individual's face). We do this to reduce the risk of threat actors impersonating you in order to access further information about you via IDCARE services (something we know impacts other organisations), or deceive IDCARE into contacting other organisations with information about you.

The facial imagery that you provide us is matched against third-party templates in a manner that does not involve the retention by that third-party of the templated biometric (ie. the measure of an individual's face). Verification involves requesting of third parties whether the biometric template IDCARE has collected about you is consistent with the biometric template and the related personally identifiable information that is held by the third-party (such as name, date of birth, driver licence or passport number and address). Third parties that receive these requests from IDCARE include Government identity credential issuers, financial institutions, telecommunications providers, and digital identity issuers and verifiers. IDCARE may deny access to specific services or request an individual to provide alternative information to assist the verification assessment if inconsistencies are found and cannot be resolved.

Sharing of personally identifiable information with third parties ("Sharing Provision")

IDCARE may share personally identifiable information with third parties, such as law enforcement, financial institutions, Government agencies (including identity document issuing agencies) and other identity repair response organisations in the following circumstances:

- where you have consented for IDCARE to share such information; and/or
- where it is assessed by IDCARE to be a situation where an individual has an immediate threat to their life (for example, a client is assessed to be at imminent risk of self-harm and IDCARE reports this instance to local law enforcement or another service provider to conduct a physical welfare check); and/or
- where IDCARE is permitted or required by law, such as if IDCARE has been issued with a subpoena, warrant or related legal request from a Court or relevant law enforcement body, or IDCARE reasonably believes the use or disclosure of the information is reasonably necessary for enforcement related activities conducted by, or on behalf of, an enforcement body.

Identity protection and alerting services

Third-parties may search against IDCARE's verification holdings where agreements are in place between IDCARE and:

- the third party and such searching is conducted in a manner consistent with this Privacy Policy and the Terms & Conditions of any relevant IDCARE service the individual has provided consent to use; or
- IDCARE is otherwise permitted or required by law, such as where it has a reasonable belief that disclosure is reasonably necessary for enforcement related activities conducted by an enforcement body.

Cost-recovered services

Services that are cost recovered are subject to their own Terms & Conditions which are consistent with this Policy. Cost recovered services may be delivered solely by IDCARE or in conjunction with a third party and requires such users to make payment and provide personally identifiable information to IDCARE in order for IDCARE to perform this service, such as name, contact details, and payment information.

Payment is made via a third-party payment processing platform. 128-bit encryption is used in the processing of such payments and at no point does IDCARE collect, store or share such payment information. Users of this service must agree to the terms and conditions of the third-party payment platform including their own Privacy Policy (a relevant link has been provided on this payment gateway).

Personally identifiable information protection

IDCARE will take all reasonable care to protect personally identifiable information provided by clients. At least annually IDCARE undertakes risk assessments in relation to our collection, storage, sharing, and destruction of personal information (guided by the ISO 31000 standard on risk management).

IDCARE operates a "defence in depth" approach to the information it collects, stores and communicates, including, but not limited to:

- All data transmitted over the internet is done over HTTPS
- Cloudflare is used extensively to block potentially malicious requests
- Rate limits on APIs are implemented at both the code level and via Cloudflare
- Regular security scans are performed to identify code or configuration vulnerabilities
- Firewalls are employed to limit access to services running on Microsoft Azure
- All handling of personal information by staff is subject to specific policies and guidelines which are reviewed regularly for compliance
- Data at rest is encrypted
- Staff are regularly assessed and educated about cyber security threats and threat responses
- Any and all investigations regarding malicious code, sites and dark net actions are performed using external networks, interfaces and unattributable settings.

Retention of personally identifiable information

You may request at any time that information IDCARE has about you be permanently deleted (see next section).

IDCARE only retains personal information for the purposes of assisting you and protecting and responding to risks relating to such information. We retain records for 7 years in accordance with best practice document retention guidelines. Case information is anonymised and retained for statistical analysis, such as time series analysis. This information is backed-up periodically and stored in a non-networked or Internet-enabled environment.

If IDCARE receives unsolicited information we will determine whether it would have been permitted to collect the information. If not we will destroy the information as soon as practicable.

Access, deletion, correction, feedback and complaints

If you wish to access information collected by IDCARE relating to your circumstances, seek correction of information held about these circumstances, have your personally identifiable information deleted, or make a complaint about how we have dealt with your matter, please send a written request, including your case number, to:

Privacy Officer IDCARE PO Box 412 Caloundra QLD Australia 4551

Requests may also be emailed using our feedback form, with the words "Attn: Privacy Officer" in the subject line accessed at www.idcare.org or by emailing direct contact@idcare.org.

To assist IDCARE in responding to your request we would be grateful if you could provide your IDCARE Case Number (if relevant) and the estimated date of your engagement with IDCARE.

If we have not resolved your issue to your satisfaction and within our responsibilities, complaints about IDCARE and the handling of your personal information may be made to the relevant Privacy Commissioners in Australia and New Zealand: (www.oaic.gov.au

/ ph: 1300 363 992 and www.privacy.org.nz / ph: 0800 803 909). These organisations have extensive materials about your privacy rights and response considerations.

IDCARE OFFICIAL POLICY