iDcare's Privacy Policy

Statement of affirmation
iDcare operates across Australia and New Zealand and vigorously supports the Australian and New Zealand privacy principles. In fact, for organisations to be an accredited member of iDcare we must assess them to also be in compliance with these principles. iDcare believes that there is an inherent relationship between on-going compliance with these privacy principles and the means by which organisations can mitigate against identity theft and misuse.

Our functions & assessing the risks
iDcare engages with individuals and organisations on highly sensitive issues involving the loss or theft of personal information. The primary Object of iDcare is to represent the individual interests of identity theft victims through a number of activities, including raising awareness, education, building the capacity of organisations to respond to identity theft and misuse events, and directly supporting victims in providing them with practical knowledge on what to do in response to an event.

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 also performs Privacy Impact Assessments when proposing the delivery of new community services to evaluate the nature of the risk, strategies for mitigation, and our on-going responsibilities in meeting Australia and New Zealand's privacy principles.

Safeguards
As a community-based organisation iDcare has implemented a number of safeguards in relation to personal information. First, iDcare does not collect or ask for personal information from our clients. In other words, we make it a point not to collect information from clients that can identify them. The information we do collect is typically limited to a person's first name (or a first name they are comfortable with providing), their postcode, and the circumstances surrounding the concerns they have or information they seek from iDcare. This is stated explicitly on our website and is reiterated during the initial engagement we have with clients over the phone or on-line.

Secondly, iDcare does not charge members of the community, our clients, for the services we perform. iDcare is an Australian registered charity. Not charging individuals for our services is another way iDcare reduces the amount of personal information it collects. It is also an active way iDcare mitigates against phishing and related threats. Phishing typically involves the unsolicited emailing of members of the public by criminals that seek to impersonate organisations and convince such individuals to share their personal information and/or part with their money.

Information iDcare does collect and share
In order for iDcare to 'close the loop' and provide relevant third parties with advice on how to enhance customer service and response capabilities, **we do seek the consent from individual clients to share their contextual information and**

experiences with third parties in order to assist broader industry, government or research efforts in preventing and responding to identity theft and misuse.

Such information can include, but may not be limited to:

- Details of specific organisations that have products or services that are believed to be involved in the identity theft and misuse event(s) (for example, a specific government agency that issues a driver's licence or birth certificate or a financial institution that provides a credit card product);
- The date and circumstances the client believes that their personal information was compromised;
- The date and circumstances the client believes that their personal information was subsequently used in further acts (if applicable);
- The amount of money and time expended in response to a client's identity theft and misuse experience;
- The amount of money and type of product or service that is alleged to have been acquired / obtained in the use of the personal information that has been compromised (for example, using stolen credit card details to purchase an airline ticket and the amount of money involved);
- Specific feedback provided by clients that are directed to third parties. iDcare's client engagement provides for our clients to communicate information that can be directed to specific third parties that have a connection with their circumstances (for example, Executives within organisations that have products and services believed to have been used in the identity theft and misuse act).

Whilst the information iDcare collects cannot enable iDcare to identify the individual client, the provisioning of circumstantial information to third parties may enable them to identify their customer. For example, if consent was provided by a client to share their circumstances with the organisation that had a product or service involved in the theft or misuse, and that organisation had only experienced one identity theft event during the period concerned, then that third party could assume that the iDcare client is a individual known to them. iDcare seeks to mitigate this risk through working closely with our network of organisations in order to understand the volume of identity theft and misuse individual organisations are experiencing prior to sharing such reporting. In instances where a network member has had one known case, iDcare will assess the risk that any non-personal information shared, even if consent has been provided, will result in that client's identity becoming known by the third party.

Our organisational network is an important feature of how iDcare maintains its knowledge of the latest response strategies that we advise our clients. It presents an opportunity for our clients to communicate via iDcare direct with executives in relevant organisations across the public and private sectors in Australia and New Zealand. iDcare continues to see positive changes made as a result of facilitating the feedback of client experiences with such organisations.

iDcare may also provide non-personal identifying information and aggregate data to research organisations, such as tertiary institutions and Centres of Excellence, in order to advance research and understanding of identity crime and related subjects. In such instances iDcare also asks the researchers to comply with the iDcare policy

on *Supporting Academic Researchers and Clinical Placements*. A copy of this Policy can be requested from the iDcare Privacy Officer.

How does iDcare obtain and record a client's consent to share information?
Consent is either obtained verbally or online (through email or webchat) and is logged on our case management system. Our case management system collects broad statistics on the nature of the identity theft and misuse case presented. Each client is provided a client number to facilitate future engagement with iDcare.

Storage of our client information
As we deal with sensitive and difficult situations and issues, we strive to keep the information we gather confidential and secure in accordance with our obligations under the Privacy Act 1993 (NZ) and the Privacy Act 1988 (Cwth).

Gathering information
iDcare's case management centre is the primary mechanism through which we collect contextual information about a client. iDcare's organisational membership network facilitates the collection of non-personal statistics and trends on identity crime. This information assists iDcare in our engagement with clients in understanding the prevalence of the circumstances they present, trends in response measures, and other analysis that can assist in preventing and responding by both individual clients and organisations.

Protection of information
iDcare's periodic risk assessments inform us of the steps we need to take and modify in keeping our information securely so that it is safeguarded against loss, unauthorised access or misuse. In the event that iDcare possesses personal information, including that of staff members and volunteers, we do not release personal information to third parties otherwise than in accordance with the Privacy Act 1993 (NZ) and Privacy Act 1988 (Cwth).Examples of circumstances where we may release personal information include (but are not limited to):

1. When the individual concerned specifically authorise it;
2. When the purpose the information was collected was so that iDcare could provide it to a third party;
3. There is a serious and imminent threat to life or health;
4. To enable law enforcement to maintain the law, including investigating offences; etc.

Access and complaints
If you wish to access information collected by iDcare relating to your circumstances, seek correction of information held about these circumstances, 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 Australia 4551

Requests may also be emailed to <yourvoice@idcare.org> with the words “Attn: Privacy Officer” in the subject line. Without citing your case number it will be difficult for iDcare to respond to your request. If you have lost this number, it would be of assistance to iDcare if you could provide the details of when you engaged with iDcare, the name of the iDcare staff member, and the broad nature of your circumstances.

Retention

iDcare only retains personal information for as long as is it is required for the purposes for which that information may lawfully be used (for example, employee and volunteer details, next of kin information etc).