PRIVACY & CONFIDENTIALITY POLICY

OTFC-GROUP

Purpose and Scope

The OTFC Group will manage and ensure that the rights of clients remain private and only used for the purpose that it is collected. This policy applies to all employees.

Any personal information held by THE OTFC GROUP is protected under the Privacy Amendment (Enhancing Privacy Protection) Act 2012.

Policy

The Privacy Act 1988 (Privacy Act) was introduced to promote and protect the privacy of individuals and to regulate how Australian Government agencies, private organisations and some other organisations, handle personal information. The Privacy Act includes 13 Australian Privacy Principles (APPs), which apply to the above organisations and are collectively referred to as 'APP entities'. The OTFC Group is an APP entity and therefore must abide by the 13 APP's stated below (links provided for full guideline)

1. APP 1 Open and Transparent management of personal information
2. APP 2 Anonymity and pseudonymity
3. APP 3 Collection of solicited personal information
4. APP 4 Notification of the collection of personal information
5. APP 5 Dealing with unsolicited personal information
6. APP 6 Use or disclosure of personal information
7. APP 7 Direct Marketing
8. APP 8 Cross border disclosure of personal information
9. APP 9 Adoption, use or disclosure of government related identifiers
10. APP 10 Quality of personal information
11. APP 11 Security of personal information
12. APP 12 Access to personal information
13. APP 13 Correction of personal information

The OTFC Group is committed to protecting and upholding the right to privacy of clients, staff, management and representatives of agencies we deal with.

The OTFC Group is committed to protecting and upholding the rights of our clients to privacy in the way we collect, store and use information about them, their needs and the services provided to them.

The OTFC Group requires employees and management to be consistent and careful in the way they manage what is written and said about individuals and how they decide who can see or hear this information.

The OTFC Group is subject to the requirements of the NDIS (Quality and Safeguards) Commission. The organisation will follow the guidelines of the Australian Privacy Principles in its information management practices.

The OTFC Group will ensure that each client understands and agrees to what personal information will be collected and why, including recorded material in audio and/or visual format.

The OTFC Group will advise each client of confidentiality policies using the language, mode of communication and terms that the client is most likely to understand.

The OTFC Group will ensure that:

- It meets its legal and ethical obligations as an employer and service provider in relation to protecting the privacy of clients and organisational personnel.
- Clients are provided with information about their rights regarding privacy and confidentiality.
- Clients and organisational personnel are provided with privacy and confidentiality when they are being interviewed or discussing matters of a personal or sensitive nature.
- All staff, management and volunteers understand what is required in meeting these obligations.
- Clients are advised of confidentiality policies using the language, mode of communications and terms that are most likely to be understood. Our company will attempt to locate interpreters and use easy access materials such as those on NDIS website.
- In the case of divorced or separated parents, we will only deal with the fee-paying party who engaged our services in the first instance. We will only share information relating to the assessment and treatment of the child with the other parent and/or carer's if we have the consent of the initial party or are legally obliged to disclose specified information under Court Order.

This policy will apply to all records, whether hard copy or electronic, containing personal information about individuals, and to interviews or discussions of a sensitive personal nature.

This policy conforms to the Federal Privacy Act (1988) and the Australian Privacy Principles which govern the collection, use and storage of personal information.

Procedures

Kinds of personal information collected and held
In performing its functions, the OTFC Group collects and holds the following kinds of personal information (which will vary depending on the context of the collection):

- name, address and contact details (e.g. phone, email and fax) of client and caregivers
- photographs, video recordings and audio recordings
- Referring Partner (teacher, GP, Paediatrician etc)
- Information about your personal circumstances (e.g. marital status, age, gender, occupation, accommodation and relevant information about your family)
- Information about your identity (e.g. date of birth, country of birth)
- Information about your occupation (school or employment)
- Information about your background (the languages you speak and your English proficiency)
- Government identifiers (e.g. NDIS Number, Medicare and Private Health Insurance Details)
- Court orders (where communication or access to the client is restricted)
- Information about assistance provided to you under the NDIS.

On occasions, the OTFC Group may collect or hold some sensitive information about you, including information about:

- Your racial or ethnic origin;
- Your health (including information about your medical history and any disability or injury you may have);
- Information about any Behaviour Support Plans or Regulated Restrictive Practice in place
- Information about any cultural or religious beliefs OTFC needs to abide by upon your visit
- Information about the supports or services you receive, including supports or services you receive or have received under the NDIS and information about the people who provide those supports or services to you

When will OTFC Group collect personal information?
The OTFC Group will usually gather personal information about children, young adults and their families:

- When a caregiver books a child in for an initial assessment
- At the time of an Initial Assessment
- During the course of providing therapeutic services
- When a child, parent or family uses the OTFC Group website (e.g. when they fill out an online form, enter a competition or subscribe to an online newsletter).

Purposes for which OTFC Group collects personal information?
The OTFC Group collects personal information in order to conduct its business, to provide and market its services and to meet its legal obligations. The Group will not use your personal data for any purpose that you have not agreed to.

The OTFC Group collects and holds personal information for a variety of different purposes relating to its functions and activities including:

- Performing its primary function of providing therapeutic and assessment services to the community
- Performing its employment and personnel functions in relation to its staff and contractors
- Performing its legislative and administrative functions
- Policy development, research and evaluation
- Complaints handling
- Management of correspondence with the public

- To process Medicare, NDIS and private health fund claims
- To supply information to medical practitioners and other allied health professionals who provide necessary follow up treatment and ongoing care
- To conduct research and development
- To conduct service planning
- To communicate offers and special events

How the OTFC Group collects and holds personal information

The OTFC Group collects personal information through a variety of different methods including:

- Paper-based forms
- Electronic forms (including online forms)
- Face to face meetings
- Telephone communications
- Email communications
- Communications by fax
- The OTFC Group website; and
- The OTFC Groups social media websites and accounts. OTFC Group collects personal information from the web site www.occupationaltherapychildren.com.au through receiving subscription applications and emails. They also use third parties to analyse traffic at that web site, which may involve the use of cookies.
- In some circumstances the OTFC Group may be provided with personal information about an individual from a third party – for example, a report provided by a medical professional or a referral from another professional

The OTFC Group holds personal information in a range of paper-based and electronic records. Storage of personal information (and the disposal of information when no longer required) is managed in accordance with the Australian Government records management regime, including the Archives Act 1983, Records Authorities and General Disposal Authorities. This ensures that we hold your personal information securely.

About whom does OTFC Group collect personal information?
The type of information OTFC Group may collect and hold includes (but is not limited to) personal information about:

- Clients
- Caregivers and other family members
- Potential clients
- Employees, prospective employees and contractors
- Student
- Volunteers
- Business associates
- Suppliers and their employees, and
- Other people who encounter a member of the OTFC Group

OTFC may disclose your personal information to:

- Other members of the OTFC Group
- Legal practitioners, courts, tribunals and regulatory authorities, and
- Anyone else to whom you authorise us to disclose it as per the Privacy Permission Form

Dealing with personal information

In dealing with personal information, The OTFC Group staff will:

- Ensure privacy for clients, staff, or management when they are being interviewed or discussing matters of a personal or sensitive nature.
- Only collect and store personal information that is necessary for the functioning of the organisation and its activities.
- Use fair and lawful ways to collect personal information.
- Collect personal information only by consent from an individual.
- Ensure that people know what sort of personal information is held, what purposes it is held for and how it is collected, used, disclosed and who will have access to it.
- Ensure that personal information collected or disclosed is accurate, complete and up-to-date, and provide access to any individual to review information or correct wrong information about themselves.
- Take reasonable steps to protect all personal information from misuse and loss and from unauthorised access, modification or disclosure.
- Destroy or permanently de-identify personal information no longer needed and/or after legal requirements for retaining documents have expired.
- Ensure that clients understand and agree to what personal information will be collected and why.
- Clients will be informed why any recordings occur – audio and/or visual format. These must be agreed to in writing.

What are our obligations when information is given "in confidence"?

When information is given "in confidence " about a client by a person other than the client (that is a request that it not be communicated to the client to whom it relates) staff must:

- In the client's medical record, record only information if it is relevant to the provision of health services to, or the care of, the client in the clinical notes or warnings in PracSuite;
- Take reasonable steps to ensure that the information is accurate and not misleading; and
- Take reasonable steps to record that the information is given in confidence and it is to remain confidential.

What strategies can we take to maintain personal privacy/confidentiality?

- Only access information if it is relevant to your work.
- Do not divulge, copy, release, sell, loan, review, alter or destroy any personal information unless it is part of your job. If it is part of your job to do any of these tasks, staff are to follow the correct OTFC Group procedure (such as putting confidential papers in appropriate security bins).
- Verbal information must be protected. All staff need to be mindful of where they carry out discussion of client care. Conversations regarding clients must not be conducted in the presence of, or be heard by, unauthorised persons.
- Client and staff information (e.g. addresses or diagnosis) must never be discussed with friends or relatives without the appropriate consent.
- Client information should only be discussed between clinical staff involved in the care and treatment of the client
- Confidentiality of information may be breached when communicating personal information. Staff should be aware of and follow the correct procedure when using the fax, phone, email addresses to communicate personal information.
- Staff should be aware of situations involving young persons, whereby the client may not want information of their condition relayed to their parent/guardian.
- All personal information for clients and staff is protected according to the OTFC guidelines. In certain circumstances clients or staff may request additional measures to protect their personal information.
- Nothing in this procedure shall prevent an employee from supplying appropriate information to the Union/Professional Body in relation to probable, threatened or actual grievance or industrial dispute.

The highest standards of confidentiality are expected within the OTFC Group. Any violations of the confidentiality procedure will be addressed through the CEO and could result in disciplinary action.

Examples of "breaches of confidentiality" include:

- Divulging personal information without consent.
- Telling a relative or friend about a client or staff member without consent
- Gossiping about clients or staff
- Reading medical records when it is not in the course of work duties.
- Discussing client information in open spaces
- Accessing diagnostic results of family, friends or co-workers.
- Accessing a medical record or components of the client record that are not required for you to do your work.
- Accessing electronic systems that you are not authorised to do so through password sharing.

Client Records

Client records will be confidential to clients and staff directly engaged in delivery of services to the client. Information about clients may only be made available to other parties with the consent of the client, or their advocate, guardian or legal representative. All client records will be kept on a securely protected database that is restricted to staff members directly engaged in delivery of service to the client.

All paper client records will be kept securely in a locked filing cabinet.

Responsibilities for managing privacy

- All staff are responsible for the management of personal information to which they have access, and in the conduct of research, consultation or advocacy work.
- The CEO is responsible for content in the OTFC Group's Services' publications, communications and website and must ensure the following:
- Appropriate consent is obtained for the inclusion of any personal information about any individual including The OTFC Group personnel (Consent policy)
- Information being provided by other agencies or external individuals conforms to privacy principles
- That the website contains a Privacy statement that makes clear the conditions of any collection of personal information from the public through their visit to the website.
- The CEO is responsible for safeguarding personal information relating to The OTFC Group staff, management, contractors.
- The CEO will be responsible for:
    - Ensuring that all staff are familiar with the Privacy Policy and administrative procedures for handling personal information.
    - Ensuring that clients and other relevant individuals are provided with information about their rights regarding privacy.
    - Handling any queries or complaint about a privacy issue.

Privacy information for clients

Prior to the initial assessment in the onboarding documentation, clients will be told what information is being collected, how their privacy will be protected and their rights in relation to this information.

Privacy for interviews and personal discussions

To ensure privacy for clients or staff when discussing sensitive or personal matters, the organisation will:

- Only collect personal information which is necessary for the provision of information provided on the site;
- Which is given voluntarily; and
- Which will be stored securely on the OTFC Group database

When in possession or control of a record containing personal information, The OTFC Group will ensure that:

- The record is protected against loss, unauthorised access, modification or disclose, by such steps as it is reasonable in the circumstances to take;
- If it is necessary for that record to be given to a person in connection with the provision of a service to the OTFC Group, everything reasonable will be done to prevent unauthorised use or disclosure of that record.

The OTFC Group will not disclose such personal information to a third party:

- Without the individual's consent; or
- Unless that disclosure is required or authorised by or under law

Third Parties

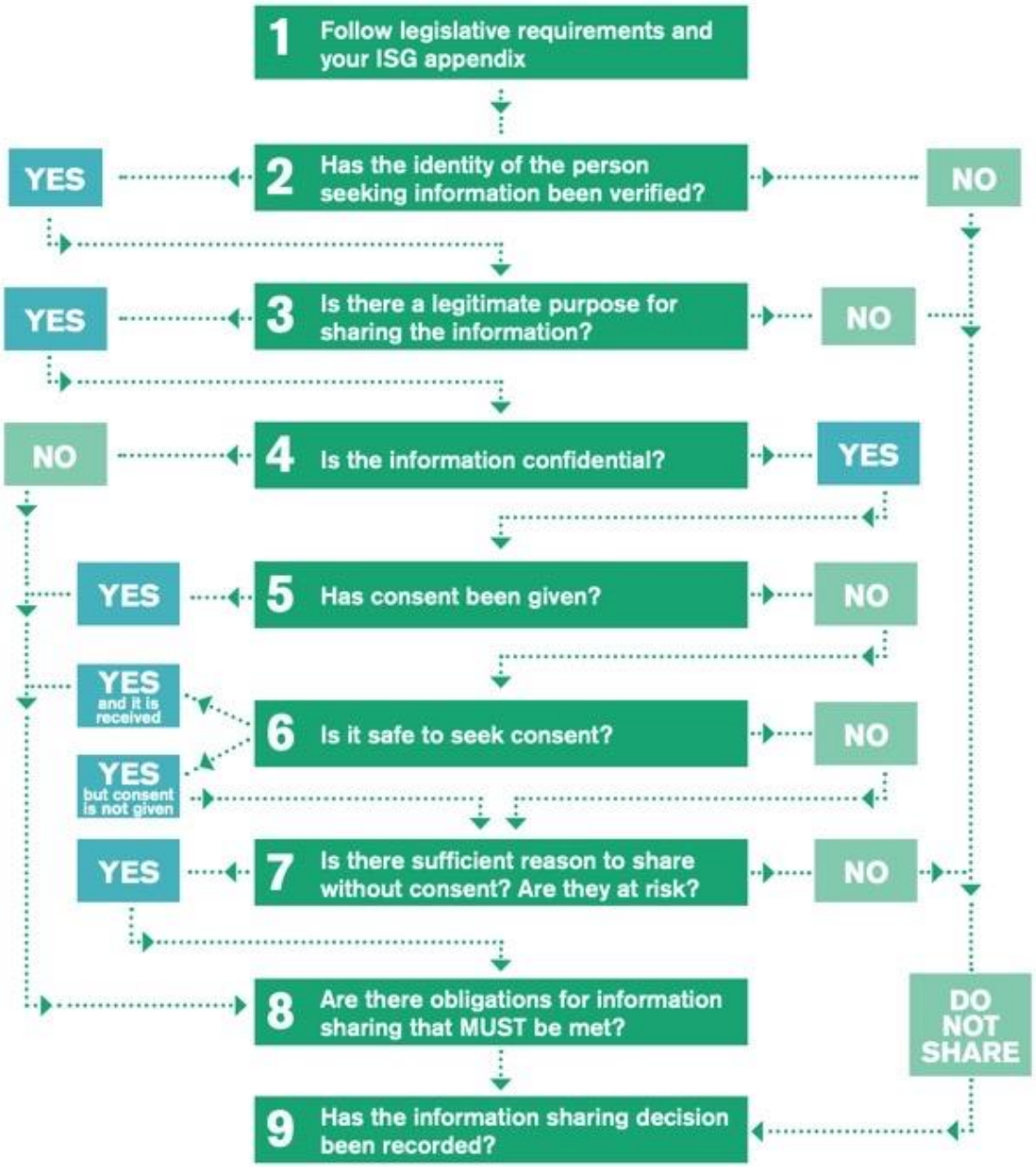
We do not and will not sell or deal in personal or client information. We will never disclose your personal details to a third party except the necessary information required by providers of products or services you have purchased or to protect the rights, property or safety of the OTFC Group, our clients or third parties or if required by law. We may however use in a general sense without any reference to your name, your information to create marketing statistics, identify user demands and to assist it in meeting customer needs generally. In addition, we may use the information that you provide to improve our website and services but not for any other use unless agreed to in writing

Sharing Information
The safety and wellbeing of people are the primary considerations when making information sharing decisions.
• Information sharing decisions are made on a case-by-case basis using best interest principles and are supported by sound risk assessment.
• Gaining a client's consent for information sharing is the ideal and recommended practice, except where to do so would place a person at risk of serious harm or where it is not practicable or reasonable to do so.
• Working in partnership with parents and other adults to provide safe and supportive family environments directly protects children's and young people's wellbeing.
• When information is shared about people, in both verbal and written communication, it is done so respectfully.
• 'Respecting cultural difference' means having the same aims for people's wellbeing and safety but finding appropriate ways of achieving them.
• An adult's wellbeing needs should not compromise a child's safety and wellbeing.

What are the grounds for information sharing?
Sufficient reason for sharing information exists if the person disclosing the information believes, on reasonable grounds, that the disclosure is necessary to:
• divert a person from offending or harming themselves
• protect a person or groups of people from potential harm, abuse or neglect
• protect service providers in situations of danger
• help service providers more effectively address risks to safety and wellbeing
• alert other service providers to a person's need for assistance.

A client's informed consent to share information must be sought in all situations where it is considered reasonable and practicable to do so. The decision to share without consent must be based on sound risk assessment and approved by the Clinical Manager of the practice. Disclosure of information without consent is permitted if it is not safe or possible to seek consent or consent has been refused and the disclosure is reasonably necessary to prevent or lessen a serious threat to the life, health or safety of a person or group of people. In certain circumstances, disclosure may be authorised or required by law and consent is not required.

ISG Decision Making Steps



If you are unsure at any stage about what to do, consult your line manager/supervisor.
If as a supervisor/line manager you are unsure and need help or advice consult the SA Principal Advisor Information Sharing at Ombudsman SA on 8226 8699 or 1800 128 150 (outside Adelaide metro).

How to seek access to and correction of personal information
You have a right under the Privacy Act to access personal information held about you. You also have a right under the Privacy Act to request corrections to any personal information the OTFC Group holds about you if you think the information is inaccurate, out-of-date, incomplete, irrelevant, or misleading. However, the Privacy Act sets out circumstances in which the OTFC Group may decline access to or correction of personal information (e.g. where access is unlawful, or where the personal information held is an opinion and not an objective fact).
To access or seek correction of personal information we hold about you, please contact jo@otfc.com.au

Accidental or unauthorised disclosure of personal information
The OTFC Group will take seriously and deal promptly with any accidental or unauthorised disclosure of personal information. The OTFC Group follows the OAIC's Data breach notification — A guide to handling personal information security breaches when handling accidental or unauthorised disclosures of personal information. Legislative or administrative sanctions, including criminal sanctions, may apply to unauthorised disclosures of personal information.

Data security
Access to personal information held within the OTFC Group is restricted to authorised persons who are staff or contractors. Electronic and paper records containing personal information are protected in accordance with Australian Government security policies.
The Practice Management System at the OTFC Group is Pracsuite (a cloud-based PMS) and is managed by Smartsoft. IP Barring exists to ensure staff cannot access client information outside of the OTFC Group IP addresses. There is also 2- Factor Authentication employed with the PMS as an extra layer of security

The OTFC Group uses Microsoft (outlook, Microsoft teams, sharepoint, onedrive) to communicate, house the client database and hold information. The OTFC Group information technology portfolio is managed by Blackbird IT who regularly conduct audits to ensure the information held electronically adheres to their protective and computer security policies. All information is backed up to a local site on Fullarton Road.

The OTFC Group website
This website is managed externally by Brain Box Media and Social Soul Media and internally by members of the leadership team involved in Marketing and Projects. OTFC Group only collects personal information from its website where a person chooses to provide that information.

Electronic communication
There are inherent risks associated with the transmission of information over the Internet, including via email. You should be aware of this when sending personal information to us by email or by using the OTFC website. If this concerns you, you may prefer to use other methods of communication with such as post, fax, or phone (although these methods have associated risks). The OTFC Group records email addresses when a person sends a message or subscribes to a mailing list. Any personal information provided, including email addresses, will only be used or disclosed for the purpose for which it was provided.

OTFC also collects personal information from these organisations and individuals and will deal with that information in accordance with this Policy.

OTFC works in partnership with a range of government departments and health services and is required by law to pass on certain information about clients. We must also adhere to the laws of Mandatory Notification, and therefore must notify relevant authorities about certain issues (e.g. child protection).

External and internal quality auditors may view a small amount of personal information to check that OTFC is meeting its obligations for Quality Accreditation. Auditors are bound by their own and/or OTFC's confidentiality requirements. Volunteers and students on placement at OTFC are also bound by OTFC's confidentiality requirements. In some cases, we share stories about OTFC families through newsletters, publications, media stories and fundraising activities. We will always seek your permission to do this and will tell you exactly where and when your story will appear.

Security
We strive to ensure the security, integrity and privacy of personal information submitted to our website, and we periodically update our security measure in light of current technologies

Links
This website may contain links to other websites. These links are meant for your convenience only. Links to third party websites do not constitute sponsorship or endorsement or approval of these websites. Please be aware that we are not responsible for the privacy practices of such other websites. We encourage our users to be aware, when they leave our website, to read the privacy statements of each and every website that collects personally identifiable information. This privacy policy applies solely to information collected by this website.

How does OTFC keep personal information accurate and up-to-date?
OTFC Group endeavours to ensure that the personal information we hold is accurate, complete and up-to-date. We encourage you to contact our admin team in order to update any personal information we hold about you. Contact details are: Jo@otfc.com.au

You can seek access to your personal information. Subject to the exceptions set out in the Privacy Act, you may seek access to the personal information which OTFC holds about you by contacting Michelle at: michelle@otfc.com.au

OTFC will require you to verify your identity and to specify what information you require. In some instances, a fee may be charged for providing access. We will advise you of the likely cost in advance.

Updates to this Policy
This Policy will be reviewed from time to time to take account of new laws and technology, changes to our operations and practices and the changing business environment.

The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government (and Norfolk Island) agencies and Australian Privacy Principle (APP) entities.

APP 11 requires APP entities to take active measures to ensure the security of personal information they hold and to actively consider whether they are permitted to retain this personal information.

Specifically, APP 11.1 states that an APP entity that holds personal information must take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

Under APP 11.2, APP entities must also take reasonable steps to destroy or de-identify the personal information they hold once it is no longer needed for any purpose for which it may be used or disclosed under the APPs. This requirement does not apply where personal information is contained in a 'Commonwealth record' or where the entity is required by law or a court/tribunal order to retain the personal information.

An entity 'holds' personal information 'if the entity has possession or control of a record that contains the personal information'. The term 'holds' extends beyond physical possession to include a record that an entity has the right or power to deal with. For example, an entity that outsources the storage of personal information to a third party, but retains the right to deal with that information, including to access and amend it, 'holds' that personal information.

When considering the security of personal information, the organisation has been mindful of other obligations under the Privacy Act, such as your obligations under APP 8 (Cross-border disclosure of personal information) and APP 12 (Access to personal information).

Data Breaches

Data breaches can be caused or exacerbated by a variety of factors, involve different types of personal information, and give rise to a range of actual or potential harms to individuals and entities. As such, there is no single way of responding to a data breach. Each breach will need to be dealt with on a case-by-case basis, with an understanding of the risks posed by a breach and the actions that would be most effective in reducing or removing these risks.

Generally, the actions taken following a data breach should follow four key steps:

Step 1: Contain the data breach to prevent any further compromise of personal information.

Step 2: Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.

Step 3: Notify individuals and the Commissioner if required. If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for the entity to notify.

Step 4: Review the incident and consider what actions can be taken to prevent future breaches.

At any time, entities should take remedial action, where possible, to limit the impact of the breach on affected individuals. If remedial action is successful in preventing a likely risk of serious harm to individuals, the NDB scheme notification obligations may not apply.

In general, entities should:

- take each data breach or suspected data breach seriously and move immediately to contain, assess and remediate the incident. Breaches that may initially seem immaterial may be significant when their full implications are assessed
- undertake steps 1 (Contain), 2 (Assess), and 3 (Notify) either simultaneously or in quick succession. In some cases it may be appropriate to notify individuals immediately, before containment or assessment of the breach occurs
- determine how to respond on a case-by-case basis. Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, an entity may take additional steps that are specific to the nature of the breach

The following diagram summarises the data breach response process. The parts of this process that are required by the NDB scheme are coloured red. The NDB scheme is explained in detail in Part 4 of this guide.

Maintain information governance and security — APP 1 and 11

Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.

Contain

An entity's first step should be to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

Entities will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, entities should consider whether **remedial action** is possible.

Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- **Initiate:** plan the assessment and assign a team or person
- **Investigate:** gather relevant information about the incident to determine what has occurred
- **Evaluate:** make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.

Entities should conduct this assessment expeditiously and, where possible, within 30 days.

If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, an entity should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

NO — **Is serious harm still likely?** — **YES**

Notify

Where **serious harm is likely**, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- **Option 1:** Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3:** publish the statement on the entity's website and publicise it

Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review

Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Entities should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- professional bodies
- your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.

Notifiable Data Breaches (NDB)

A data breach happens when personal information is accessed or disclosed without authorisation or is lost. If the Privacy Act 1988 covers your organisation or agency, you must notify affected individuals and us when a data breach involving personal information is likely to result in serious harm.

When an organisation or agency the Privacy Act 1988 covers has reasonable grounds to believe an eligible data breach has occurred, they must promptly notify any individual at risk of serious harm. They must also notify the OAIC by completing the following form:
https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB

An eligible data breach occurs when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by an organisation or agency (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- The organisation or agency has been unable to prevent the likely risk of serious harm with remedial action.

Feedback and complaints

Enquiries

If you have any questions about privacy-related issues please contact the CEO on 08 8410 4522 or via email on michelle@otfc.com.au. Within five working days of receiving your inquiry, a member of the leadership team will:

· discuss your complaint with you

· discuss the resolution you require and the available remedies

· where appropriate, put in place an agreed solution that meets the requirements of National Privacy Principles

· provide written notice to you of the outcome.

How to make a complaint

If you think the OTFC Group may have breached your privacy rights, you may contact us using the contact details set out at section below. The OTFC Group will respond to your complaint or request promptly if you provide your contact details. The group is committed to the quick and fair resolution of any complaints and will ensure your complaint is taken seriously. You will not suffer negative treatment if you make a complaint. The group is committed to improving the health and well-being of our clients by providing outstanding care in a modern, innovative and supportive environment. Feedback about our clients' experiences provides valuable information about what we are doing well, and where we can do things better. Please let us know about your experiences, because we really do value your opinion.
We encourage you to provide the organisation with feedback.

At OTFC we believe that feedback can help us provide you with a better service so if you are unhappy with the service or care you are receiving, you have the right to provide this feedback and feel confident in doing so.

Managing a Direct Complaint
Every complaint is different. There are no hard and fast rules to follow. The following principles will help in most situations.

- Respond promptly
- Ask Questions
- Gather all the relevant information
- Keep clear and accurate records
- Emphasise confidentiality and privacy
- Plan meetings and stay calm
- Keep your promises
- Seek advice and assistance if you are unsure about how to proceed

https://www.hcscc.sa.gov.au/for-service-providers-addressing-complaints/managing-a-direct-complaint/#clear-accurate-records

What if I do not feel that my complaint has been resolved?
If you feel that your complaint has not been resolved you may wish to contact the Health and Community Services Complaints Commissioner for further assistance (Details below)

Complaints commissioner details
Post: PO Box 199, Rundle Mall, Adelaide SA 5000
In Person: L4 East Wing, 50 Grenfell Street, Adelaide SA 5000
Telephone: 1800 232 007
Email: info@hcscc.sa.gov.au
Online Form: https://www.hcscc.sa.gov.au/making-a-complaint/raise-a-complaint-with-hcscc/

You can read details of the Privacy Act on the Australian Government Office of the Privacy Commissioner's website at www.privacy.gov.au.

Privacy Policy updates
The OTFC Group reviews this Privacy Policy regularly and update it as required.

OTFC Contact Details:

Corporate Services: Joanne Cavallaro – jo@otfc.com.au – 8410 4522

CEO: Michelle Mennillo – michelle@otfc.com.au – 8410 4522