Level 2
109 Anglesea Street
PO Box 1319
Hamilton 3204
Phone: (07) 839 0770
Fax: (07) 839 5158
Email: reception@clwaikato.org.nz

PRIVACY POLICY

POLICY & PROCEDURE

This document sets out policy and procedure.

Reference may be made to additional and separate policies for example the *Health and Safety Manual.*

The policy and procedure contained herein and in all other separate codes apply to ALL EMPLOYEES, VOLUNTEERS, and where applicable other individuals or contractors performing work.

Best efforts have been made to cover all scenarios however should a situation arise which is not covered prescribed (or requires update) please approach Management.

IMPORTANT NOTE: a breach or breaches of CLW policy may be deemed as misconduct and disciplinary action may follow.

CONTENTS

1. PURPOSE & PRINCIPLES

- The purpose of this policy is to create a shared understanding and commitment to a positive privacy culture and an effective / practical privacy framework.
- The above objective is important to ensure compliance, risk management and ultimately relationships built on trust and respect.
- This policy provides a practical guide to ensure compliance (as far as reasonably practicable) with privacy principles including but not limited to the Privacy Act, the Lawyers and Conveyancers Act, and Lawyers Conduct and Client Care Rules.

3. SCOPE

- This policy applies to all CLW "workers" which includes employees, governance, volunteer caseworkers and assistants, and any other individuals or entities that undertake work at or for CLW.
- This policy covers all operational processes (whether electronic or otherwise).
- This policy covers all "personal information" that is collected or created by CLW and it's "workers" in the course of carrying out a lawful function or CLW related business. The Privacy Act defines "personal information" as "information about an identifiable individual…which includes a natural person other than a deceased person". There are some exceptions around deceased persons.

4. ROLES & RESPONSIBILITIES

- As outlined above, all CLW "workers" are responsible for meeting the objectives of privacy as well as strict compliance with policy and procedure as stipulated herein.

PRIVACY OFFICER(S)

- The Privacy Act requires every agency / organisation to appoint a privacy officer(s). CLW will elect one or more privacy officers in accordance.
- Privacy officers are responsible for compliance, dealing with requests, responding to breaches and investigations, risk assessment and preventative action.

5. TRAINING & SUPPORT

- CLW undertakes to provide the necessary training and support to ensure that all "workers" have a clear understanding of the policy and practical application.
- All "workers" must receive a copy of this policy along with the necessary training as part of their induction at CLW. This training will include aspects on what is "necessary", collection process, factors that trigger mandatory disclosure, and practical application of privacy in and out of the office.

- Management / privacy officer(s) are responsible for ongoing review, training and support.

5. INFORMATION PRIVACY PRINCIPLES

- All agencies holding personal information about individuals have to comply with the Privacy Act.
- There are 13 Information Privacy Principles at the core of the Privacy Act. These IPPs set out how agencies are to:
    - collect personal information (IPPs 1 to 4)
    - store personal information (IPP 5)
    - provide access to (IPP 6) and correct (IPP 7) personal information
    - use (IPPs 8 and 10) and disclose (IPP 11 and 12) personal information
    - only keep personal information for as long as necessary (IPP 9)
    - use unique identifiers (IPP 12).

- A breach of any of the IPPs can have significant consequences even if there isn't a complaint to the Privacy Commissioner or an interference with privacy (i.e. a breach which causes harm to an individual as set out in the Privacy Act). Whether or not an action (or omission) in question is deemed to be a breach, will depend on the circumstances of a particular case.

PURPOSE OF COLLECTION OF PERSONAL INFORMATION

- CLW workers may collect personal information only for a lawful purpose such as the function of providing legal services.
- CLW workers may collect only information necessary to carry out a lawful function (never collect any information which on the basis that it may or may not be necessary). IF in doubt, a CLW worker must approach Management for directions.
- *TIP: if you are able to explain to the person whom you are collecting the information from exactly why the information is necessary and how it will be used it is likely that it complies with this IPP.*
- Letters of engagement must be clear about what instructions are received and Privacy Waivers must be clear about what information is sought.
- Information requested for one purpose must NOT be used for another purpose unless an exception applies for example the person concerned authorises it.

MANNER OF COLLECTION & SOURCE OF PERSONAL INFORMATION

- PRIOR to collection of personal information, the person concerned must be informed of a number of aspects. This disclosure is delivered through the *CLW Privacy Statement*, the *CLW Client Information (LCA)*, and *the CLW Terms of Engagement*.
- Prior to collecting personal information, a CLW must ensure that the individual concerned has given written instructions / consent (a standard template must be used). This authority must be clear about what permission is sought (from whom and what).
- Personal information must be collected directly from an individual concerned unless that is not practical to do so AND in which case the individual has authorised (as above).
- Collection of personal information must be carried out in a manner that is respectful, doesn't intrude unreasonably upon personal affairs and is not by unlawful means.

USE AND DISCLOSURE OF PERSONAL INFORMATION

- CLW may only use personal information for the purpose it was collected for (unless an exception applies). Hence the importance of written instructions / authority.
- CLW must ensure that disclosure of personal information to anyone other than the person concerned is in connection with the purpose of which it was obtained AND disclosure is authorised (unless an exception applies).
- A common exception to the general rule of authorised disclosure is in relation to threats of serious crime or serious threats to health and safety of anyone including the individual concerned (self-harm). Mandatory disclosure in such instance (and other circumstances which may equally qualify) must be consistent with a range of laws such as the *Lawyers and Conveyancers Act*, *Conduct and Client Care Rules 2008*, and the *Privacy Act*.
- The decisions around mandatory disclosure / reporting is a legal test which must be applied by an experienced legal practitioner.
- All employees, volunteers and individuals providing services who identify a need for mandatory disclosure (or a request from another agency as the case may be) must advise the Legal Services Manager immediately or in their absence the General Manager.
- The applicable Manager will consult with the person(s) who identified or raises the matter.
- The Manager may take advice from a CLW Trustee who is qualified to practise on their own account and or any other point of contact deemed necessary. This may include an insurer.
- In the event that a disclosure / reporting decision cannot be made within 2 hours, the Manager must explore whether interim steps can be taken to ensure the safety of everyone concerned.
- Imminent threats to safety of anyone including the individual him or herself, must be dealt with in accordance with the CLW Health and Safety Procedure.
- Client-related information may be used for statistical or research purposes but all identifying information must be removed.
- NOTE that disclosure of personal information to an organisation outside New Zealand is bound by specific principles. CLW may only disclose information in such instance IF the receiving organisation is subject to the Privacy Act because they do business in New Zealand and / or is subject to privacy laws that provide comparable safeguards to the Privacy Act and / or agrees to adequately protect the information and / or is binding scheme or laws of a country prescribed by the New Zealand Government. If none of these criteria apply, an individual may still consent as long as they have been advised of the risk of non-protection.

STORAGE AND SECURITY

- CLW must keep all personal information safe from loss and unauthorised access / interference / use.

To do so CLW must take all steps reasonably practicable which includes:

- Having an ITC policy in place that covers all aspects related to technology and communication devices.
- Instructing a trusted and experienced IT provider.
- Ensuring that all electronic information is secure, password protected and or encrypted.
- Ensuring that all paper records are secure AND destroyed securely.

- Ensuring that CLW ITC and personal devices used for work has adequate antivirus protection and portable devices have encryption measure in event of loss/theft.
- Electronic information is backed up off site and secure.
- Ensuring that all workers are aware of and adopt a process to prevent inadvertent disclosure of information via email or in paper (mail and photocopied documents).
- Ensuring that all workers comply with access permissions / settings and a risk management process is in place to prevent unauthorised access.
- Ensuring that adequate Cyber / ITC insurance cover is in place.

- CLW has a duty to ensure that personal information is accurate, up to date, and not misleading.
- CLW has a duty to ensure that personal information is stored in a manner which is organised and readily identifiable and retrievable.
- A breach(es) or potential breach(es) must be reported to management immediately. See process below.
- Specific provisions for workers:

    - Respect personal information about others as you'd expect of your own.
    - Do NOT access, use or disclose personal information in a manner which you are not authorised to or is unlawful.
    - Personal information must be stored / saved only on the CLW network (USB exception below) and in compliance with the CLW ITC policy. Under no circumstances may personal information be transferred to a personal device or the web (for example via email).
    - All devices that store personal information must be password protected.
    - Do NOT disclose your network or outlook password to anyone AND do NOT ever write it down (or email it).
    - Make sure you comply with policy regarding screen saver locks, antivirus protection on personal devices, email and phising scam avoidance, and VPN connection for remote access.
    - Make sure that personal information is saved in a SINGLE location for each separate matter (all emails, txt messages, file notes, disclosure, research should be in one location).
    - Do NOT duplicate electronic files – they should be transferred from one location to another (in terms of administration of electronic system).
    - Don't use outlook 365 as a storage platform – it has limited recoverability in the event of data loss (it also breaches the policy about keeping electronic records in one place).
    - Avoid emailing high risk data – use a secure document transfer facility as approved by Management.
    - Always check documents (electronic and hadrcopies) before distributing it. Check scanned items and photocopied material to ensure it doesn't inadvertently contain non related material.
    - Avoid retention of original documents – where possible scan and return originals to the supplier. Exceptions apply for example certain immigration documentation.
    - We have a fireproof facility onsite. A nominated person(s) has the access code and is responsible for accommodating access.

- NO documentation / files will be taken offsite unless for practical reasons or with management consent. Practical situations include for example attending mediations / court / outreach clinics. Where this applies, client confidentiality must be maintained which includes ensuring that documentation / files are secure (for example not leaving documentation / files in a parked vehicle or unattended at an outreach clinic).
- Do not use a USB for recording, storing or transfer of information UNLESS it is a CLW encrypted / password safe device.
- Make sure that paper versions of personal information is secure in the office (lock it and keep desk spaces clear – use interview rooms for all meetings).
- Reception must ensure that paper versions of personal information is secure at all times (including mail, drop offs and pick ups, registrations received, any other documentation to be processed).
- Personal information created for example file notes must be professional and factual – do not record unprofessional inferences or add adjectives /opinions.
- Be mindful of privacy at all times (don't yell across the office; find a private space to discuss matters with clients / public)

UNIQUE IDENTIFIERS

- CLW may use unique identifiers for client query management / administration. These identifiers are necessary to allow effective implementation and use of a client management system.
- Identifiers are unique to CLW and assigned only to individuals with a clear identity.
- No two individuals may share a unique identifier (although an individual may have multiple identifiers for separate client queries).

ACCESS AND CORRECTION

- Individuals who's personal information is held by CLW have a right to access personal information (unless an exemption applies) AND a right to request correction of personal information if released.
- A request for access to personal information may be actioned ONLY by lawyers or management. Lawyers must seek guidance from Management where they are unsure.
- NOTE there are important compliance provisions in relation to access requests / release / refusal for example time frames, reasons for refusals, identification, and records /proof of release / refusals.
- Where reception receive a request for access to personal information it must be referred to either a lawyer or Management ASAP and within 24 hours (urgency may require a faster response)
- CLW has standard templates for release that must be used at all times.

DESTRUCTION

- CLW is responsible to ensure that personal information is NOT kept for longer than necessary.
- Client records are retained for a period of 10 years (once instructions are complete).
- All Terms of Engagement include a provision whereby a client consents to destruction. All originals must be returned to the client as soon as practicable (which may be during the course of instructions or immediately upon completion).
- All other personal information including employee / volunteer records and company records are retained for a period of 10 years (or longer in the case of some company records).

- A table is circulated to all staff that outlines the process for information and record management (it includes responsibility assignment and access /restrictions /destructions). ALL CLW workers must understand the application in their day to day roles. This table may be updated from time to time as needed.

6. THE LAWYERS AND CONVEYANCERS ACT & CONDUCT AND CLIENT CARE

- The obligations pursuant the LCA and CCCR are in many ways consistent with the Privacy obligations pursuant the Privacy Act. However, where there are inconsistencies, the LCA will prevail (section 7 of the Privacy Act).

DUTY OF CONFIDENCE

- The *Lawyers and Conveyancers Act* and *Conduct and Client Care Rules* require lawyers to protect and hold in strict confidence all information concerning a client which is acquired in the course of the professional relationship.
- Information acquired in the course of the professional relationship that is widely known or a matter of public record will nevertheless be confidential.
- A lawyer's duty of confidence commences from the time a person makes a disclosure to the lawyer in relation to a proposed retainer (whether or not a retainer eventuates).
- The duty of confidence continues indefinitely after the person concerned has ceased to be the lawyer's client.
- Following the death of a client or former client, the right to confidentiality passes to the client's personal representatives.

TERMS OF ENGAGEMENT

- A lawyer must take all reasonable steps to ensure the client understand the nature of a retainer including aspects regarding collection and use of personal and confidential information.

DISCLOSURE OF INFORMATION TO A CLIENT

- A lawyer must promptly disclose to a client all information that the lawyer has or acquires that is relevant to the matter in respect of which the lawyer is engaged by the client.
- A lawyer is not required to disclose information to the client if the client has given informed consent to the non-disclosure of particular information; or the disclosure would be likely to place at risk the health (including mental health) or safety of the client or any other person; or disclosure would be in breach of law or in breach of an order of the court; or the information relates to a proposed retainer that the lawyer has declined.
- A lawyer must not agree to receive information on the basis that it will not be disclosed to his or her client unless the client has given informed consent to this.
- An undertaking by a lawyer to a third party (whether another client or not) to keep information confidential does not relieve the lawyer of the duty to disclose that information to the client unless the client has given his or her informed consent to the undertaking.

DISCLOSURE OF INFORMATION TO ANOTHER

- A lawyer may disclose confidential information where:

- the client (or a former client) consents / authorises; or
- the information relates to the anticipated or proposed commission of a crime that is punishable by imprisonment for 3 years or more; or
- the lawyer reasonably believes that disclosure is necessary to prevent a serious risk to the health or safety of any person; or
- disclosure is required for the purpose of a complaint against another lawyer; or
- disclosure is required by law, or by order of a court, or by virtue of the lawyer's duty to the court; or
- it is necessary to protect the interest of the client where due to incapacity the client is unable to effectively protect his or her own interest; or
- the lawyer reasonably believes that the lawyer's services have been used by the client to perpetrate or conceal a crime or fraud and disclosure is required to prevent, mitigate, or rectify substantial injury to the interests, property, or reputation of another person that is reasonably likely to result or has resulted from the client's commission of the crime or fraud; or
- disclosure is necessary for the lawyer to seek guidance from another lawyer in respect of a proper course of professional conduct, and in such case that other lawyer is bound to maintain the confidence of the client or;
- disclosure is necessary for the effective operation of the lawyer's practice including arranging insurance cover or collection of professional fees; or
- disclosure is necessary to answer or defend any complaint, claim, allegation, or proceedings against the lawyer by the client.

- *Where a lawyer discloses information under these exceptions rule, it must be only to an appropriate person and only to the extent reasonably necessary for the required purpose.*
- As per the provisions outlined in the Privacy Principles above, the decisions around mandatory disclosure / reporting is a legal test which must be applied by an experienced legal practitioner.
- All employees, volunteers and individuals providing services who identify a need for mandatory disclosure (or a request from another agency as the case may be) must advise the Legal Services Manager immediately or in their absence the General Manager.
- The applicable Manager will consult with the person(s) who identified or raises the matter.
- The Manager may take advice from a Board member who is qualified to practise on their own account and or any other point of contact deemed necessary. This may include an insurer.
- In the event that a disclosure / reporting decision cannot be made within 2 hours of concerns being raised, the Manager must explore whether interim steps can be taken to ensure the safety of everyone concerned.

USE OF INFORMATION

- A lawyer must not use information that is confidential to a client (including a former client) for the benefit of any other person or of the lawyer.
- A lawyer must not breach or risk breaching a duty of confidence owed by the lawyer that has arisen outside a lawyer–client relationship, whether to benefit the lawyer, a client, or otherwise. In such a case the lawyer must not act for a client against a person in respect of whom confidential information relevant to the matter in issue is held.

- A lawyer has an absolute duty of honesty to the court and must not mislead or deceive the court.
- A lawyer who acts for a party in a proceeding must, to the best of the lawyer's ability, ensure that discovery obligations are fully complied with by the lawyer's client and that the rules of privilege are adhered to. A lawyer must not continue to act if, to the lawyer's knowledge, there has been a breach of discovery obligations by the lawyer's client and the client refuses to remedy that breach.
- A lawyer acting for a litigant must advise the client of the scope of the client's obligations in respect of discovery, including the continuing nature of those obligations up to and including the time of final judgment, and that discovered documents may be used only for the purposes of the litigation and not for any other purpose. The lawyer must, to the best of the lawyer's ability, ensure that the client understands and fulfils those obligations.
- A lawyer must not claim privilege on behalf of a client unless there are proper grounds for doing so.
- A lawyer must not, other than by application to the court, seek to obtain on behalf of a client information or documents that the lawyer knows to be privileged unless every person holding that privilege, after having been advised of the existence of the privilege and consequences of waiver, waives that privilege.
- If a lawyer becomes aware that privileged information or documents have been inadvertently released in circumstances where privilege has not been waived, the lawyer must not disclose the contents of the material to a client, must inform the other lawyer (or litigant if unrepresented) of the release, and must return any documents forthwith.

7. PRIVACY / DATA BREACHES

- A data breach is when there is unauthorised or accidental access to or disclosure of personal information.
- Data breaches happen in a number of ways including through loss or theft, improper recycling / disposal of hard drives, hacking and improper use or disclosure, or accidental transmission of information to the wrong person.
- It is vital to any organisation's reputation and its relationship with the people who trust it with their information that it does everything it can to prevent a data breach from happening. But when a data breach occurs, it is important to do everything it can to minimise the harm that it might cause.

IDENTIFICATION AND REPORTING OF A DATA BREACH

- CLW workers must notify Management of any suspected or actual data breach(es) immediately. The quicker a response plan is put in place the better the chances are of minimising harm / loss.
- CLW adopts an absolute "no blame" approach in respect to inadvertent or accidental data breach(es).

MANAGEMENT ASSESSMENT AND NOTIFICATIONS

- In the event of a suspected or actual data breach, Management is (without delay) responsible for:
    - Containing the breach and assessment
    - Risk Evaluation
    - Notification where deemed appropriate / mandatory
    - Reflection and prevention strategy

- The steps above include immediate inquiry about how, where and what, AND taking steps to contain or prevent further breach. This may include immediate instructions to an IT provider.
- Once more detail is available about the cause of the data breach and nature, the appropriate cause of action must be mapped out.
- Management must inform the Insurer (if applicable), the Police (if applicable), and the Privacy Commissioner (if applicable) and the CLW Chairperson as soon as practicable.
- Assessment of whether there is a need to notify and whom, requires consideration of the scope of a potential or actual breach, type of personal information in question, and the risk of harm (type) that may result from a breach.
- There is no "one size fits all" approach when it comes to notification – it depends on the circumstances. Even if notification is not deemed mandatory it may still be preferred.
- In a situation where Management deem notification necessary, the CLW Board of Trustees must authorise the disclosure. The Board's decision must be made in light of full information including direction / advice from the Office of the Privacy Commissioner.
- The manner of a notification again depends on the circumstances, however direct contact by phone or email is essential unless impractical.
- At the appropriate time, Management will complete a 'reflection & correction' report for all data breaches. The report must canvas the source or cause of a breach(es), the identified weaknesses, and any 'corrective' or 'preventative' measures put in place. This may include but is not limited to physical and technical security, policy, training and third party service provider due diligence.