

Privacy Policy

Contents

Purpose of the policy	3
Policy statement	3
Definitions	3
Context for managing personal information	3
Privacy Principles	4
Collection of personal information	4
Storage of personal information	4
Use of personal information	4
Disclosure of personal information	5
Requests to access or correct personal information	5
TTPCA Privacy Officer	5
Implementation	6
Relevant Resources.....	6
Legislative Framework.....	6
TTPCA Privacy Procedures	7
Prisoners	7
Collection of information from prisoners	7
Collection of information in the provision of individual pastoral care to prisoners..	7
Collection of information in the provision of group services	7
Collection of information relating to prisoner behaviour incidents	8
Collection of information relating to TTPCA investigation processes	8
Collection of information from prisoners who are cognitively impaired	8
Storage of prisoners’ personal information	8
Destruction of personal information about prisoners	8
Use of prisoners’ personal information	9
Disclosure of prisoners’ personal information.....	9
Volunteers	11
Collection of volunteers’ information	11
Storage of volunteers’ personal information	11
Use of volunteers’ personal information	12
Disclosure of volunteers’ personal information	12
Staff and prospective staff	12
Collection of personal information during staff recruitment.....	12
Collection of personal information from staff during employment	13
Storage of personal information during recruitment	13
Storage of personal information about staff during employment	13
Use of personal information during recruitment and employment.....	13
Disclosure of personal information during recruitment and employment.....	14
Requests to access or correct personal information	14
Procedure for responding to requests to access or correct personal information ..	14

Handling breaches of privacy and complaints15
 Privacy breaches15
 Procedure for assessing harm from privacy breaches.....15
Privacy Complaints15
 Procedure for handling complaints15

Appendices

Appendix 1 : Security Measures to Safeguard Personal Information 17
Appendix 2 : Privacy Breach Incident Form 19

Purpose of the policy

1. The purpose of the policy is to provide guidance on how to manage personal information about prisoners, staff and volunteers within TTPCA.

Policy statement

2. Tira Tūhāhā Prison Chaplaincy Aotearoa (TTPCA) is committed to protecting the personal information and individual privacy of everyone who comes in contact with the organisation. This protection extends to the collection, storage, use, access to, correction, and disclosure of personal information, in accordance with the Privacy Act 2020 (the Act).
3. TTPCA aims to ensure staff and volunteers:
 - understand and comply with legal requirements for handling personal information;
 - protect people's privacy rights;
 - are aware of appropriate privacy procedures in relation to all work based practices; and
 - can appropriately respond to concerns from people about the personal information collected by TTPCA.
4. TTPCA expects all Board members, staff, and volunteers to adhere to the principles and procedures set out in this policy. To enable TTPCA to meet its legal obligations under the Privacy Act, Board members, staff and volunteers should stay up to date with this policy and any other updates from the Privacy Officer about their responsibilities.
5. This policy applies to all personal information collected, held, shared, and used by TTPCA staff and volunteers about other staff TTPCA staff¹, volunteers, and/or paihere (prisoners).

Definitions

6. This policy uses the term "staff" to refer to all paid employees and contracted staff of TTPCA and the Catholic Diocese. "Volunteers" of TTPCA are unpaid and include Board members, assistant chaplains, pastoral visitors, and general volunteers who are members of volunteer teams. The term "prisoner" encompasses prisoners in prisons run by and Ara Poutama Aotearoa (the Department of Corrections) or Serco New Zealand Limited.
7. Personal information is any information that tells us something about a person. It is not limited to "secret" or "sensitive" information, nor does it have to name the person to be "personal". Information should be considered personal if it identifies a person in some way (such as stating their address and/or health condition), or if there is a reasonable chance their identity could be pieced together based on the information.

Context for managing personal information

8. Within TTPCA, the collection and use of personal information may occur during:
 - day-to-day participation by prisoners in voluntary group spiritual/religious activity;
 - the provision of ministry to individual prisoners; and;
 - recruitment and management of staff and/or volunteers.

¹ This includes potential staff during recruitment activities.

9. TTPCA's overall approach to privacy is underpinned by, and aligned with the Act, which governs how organisations and businesses can collect, store, use and share personal information. The Information Privacy Principles in the Act are embedded in this policy.

Privacy Principles

TTPCA's approach to collecting, handling and using personal information is governed by the privacy principles outlined in the Privacy Act 2020. An overview of these principles is presented below while the specific TTPCA practice in relation to these principles is documented in the TTPCA Privacy Procedures starting on page 7.

Collection of personal information

10. Generally, information should only be collected when it is needed for a specific purpose that requires the collection of personal information. Whenever staff or volunteers obtain personal information, either directly or indirectly, they are collecting it. Staff and volunteers should carefully consider why personal information needs to be collected before asking for it.
11. Staff and volunteers should be open with a person about how their personal information will be handled and help them to understand:
 - why their personal information is needed
 - what it will be used for
 - who it will be shared with
 - what will happen if the information isn't provided
12. However, the collection of personal information is not dependent on a person consenting to it if there is a lawful purpose for doing so.

Storage of personal information

13. TTPCA will use reasonable safeguards to protect personal information from loss, and unauthorised access, misuse, modification, or disclosure. Appendix 1 highlights the security measures in place to safeguard personal information.
14. TTPCA will only hold personal information for as long as it is needed and will securely destroy information when it is no longer needed. The timeframe may differ depending on the context in which the personal information has been collected. Staff should refer to the Privacy Procedures section for guidance on the secure destruction of personal information.

Use of personal information

15. Personal information should generally only be used for the purposes for which it has been collected. TTPCA may use it in ways that are directly related to the original purpose for which it gathered the information. TTPCA may, however, use this information in another way if the person the information is collected from gives permission for the information to be used in this way.

Disclosure of personal information

16. There are limited circumstances when personal information can be shared for reasons other than for the purpose it was collected. For example, if:
- the person who the information is about gave permission for it to be shared;
 - the information will be used in a way that does not identify the person concerned;
 - sharing it is necessary to avoid endangering someone's health or safety;
 - sharing it is necessary to uphold or enforce the law; and/or
 - sharing it is one of the purposes for which the information is collected, for example, to update partner agencies on a quarterly basis.
17. The Privacy Act allows agencies to share personal information with another agency when it is necessary to prevent or lessen a serious threat to a person's safety. Please refer to the Privacy Procedures section in this document for more information.
- Personal information can only be sent to someone overseas if the information will be adequately protected or if the individual concerned gives permission. However, this is overridden when the purpose is to uphold or enforce the law, or to avoid endangering someone's health or safety.

Requests to access or correct personal information

18. Everyone has the right to request access to their own personal information or ask that information about them be corrected if they think it is wrong. The TTPCA Privacy Officer is responsible for responding to these requests.
19. A request does not need to be in writing, however best practice is to ask for the request to be made in writing or to make a note of the request to give to the Privacy Officer. This reduces the risk of disputes about the request in the future.
20. The procedure for responding to requests to access or correct personal information is highlighted in the Privacy Procedures section of this document.

TTPCA Privacy Officer

21. The Privacy Officer for TTPCA is the Chief Executive, who is responsible for:
- a) understanding the Information Privacy Principles in the Privacy Act and encouraging TTPCA to comply with the Act;
 - b) dealing with requests made to TTPCA for access to, or correction of, personal information;
 - c) notifying the Office of the Privacy Commissioner and any affected people of a privacy breach that has either caused, or it likely to cause, anyone serious harm; and;
 - d) where applicable, working with the Office of the Privacy Commissioner during the investigation of any complaints involving TTPCA.
22. Where the Chief Executive is absent, the Senior HR Advisor is responsible for undertaking the Privacy Officer duties.

Implementation

23. New staff and volunteers are made familiar with this policy as part of their induction process. Existing staff will be reminded of their obligations under this policy and the Privacy Act by the Privacy Officer at their discretion.
24. The Chief Executive of TTPCA is responsible for the maintenance of this policy.

Relevant Resources

- TTPCA Chaplains IOMS Access and Use policy
- TTPCA Employment relations policy
- TTPCA Report of Concern policy
- TTPCA Social Media policy
- TTPCA Media policy
- Corrections commitment to privacy on the Department of Corrections website

Legislative Framework

- Privacy Act 2020
- Corrections Act 2004
- Employment Relations Act 2000

TTPCA Privacy Procedures

The following privacy procedures cover personal information around the following three groups of people:

- Prisoners
- Volunteers
- Staff

Prisoners

Collection of information from prisoners

Staff and volunteers are only allowed to collect personal information from prisoners within the context of offering them individual pastoral care, faith-based studies, worship and managing incidents. The collection of personal information must always be done overtly and transparently.

Collection of information in the provision of individual pastoral care to prisoners

When chaplains undertake one-on-one pastoral care sessions with prisoners, the following personal information is collected for recording securely in TTPCA's ā-kanohi referral management tool:

- The prisoner's name
- The prisoner's record number (PRN)
- Prison unit and location of the prisoner
- Ethnicity
- Gender
- Age range
- Religion (if known)
- Name of the TTPCA staff member who engaged with the prisoner
- The general subject that was discussed will also be recorded - this will be chosen from a standard list of pastoral topics.

Note: Chaplains should make prisoners aware that this information is being collected.

During the course of one-on-one pastoral care engagements, chaplains should apply the principle of data minimisation if they capture notes about prisoners – the notes should primarily pertain to the list of personal information requirements (above) and may also include any scheduling reminders.

The purpose for collecting this personal information is so that TTPCA can report to its stakeholders on the services that have been provided and can review and improve its services to all prisoners.

Collection of information in the provision of group services

Documents containing the names (and PRNs) of prisoners who attend group faith-based studies and worship (and the date of attendance) will be collected. The purpose for collecting

this personal information is so that TTPCA can report to its stakeholders on the services that have been provided and can review and improve its services to all prisoners.

Collection of information relating to prisoner behaviour incidents

Where there is an incident of prisoner misconduct, chaplains will document this incident in their next weekly chaplaincy team meeting, raise the incident in the monthly site management meeting and report it in the monthly TTPCA reporting. The personal information collected about the prisoner will be their initials and their prisoner record number (PRN). The full name of the prisoner will not be collected for reporting purposes.

Collection of information relating to TTPCA investigation processes

Where there is an investigation which requires a TTPCA employee (or delegated authority) to interview a prisoner in relation to a concern or complaint raised about a chaplain or volunteer, the personal information collected about the prisoner will be their initials and their prisoner record number (PRN). The full name of the prisoner is not collected for reporting purposes.

Collection of information from prisoners who are cognitively impaired

Chaplains need to be sensitive to the needs of prisoners who are cognitively impaired or disabled (particularly those who are in the at-risk units) when collecting information and informing them of their privacy rights. Prisoners should also be informed of who, in the prison staff, can support them to make a request for their personal information from TTPCA, should they want to access it.

Storage of prisoners' personal information

The personal information obtained in the course of one-on-one pastoral care sessions is stored in ā-kanohi referral management tool (RMT). This database can only be accessed by authorised personnel.

All personal information in physical formats (such as notebooks) should be stored in a secure cabinet onsite at the end of each shift to protect against unauthorised access.

Documents containing the names and PRNs of prisoners who attend group faith-based studies and worship (and the date of attendance) should be stored securely.

Where personal information has been recorded about prisoner behaviour incidents, this information will be stored securely in meeting minutes and reports.

Where personal information of a prisoner has been recorded in relation to a TTPCA investigation, that information will be stored in a private directory in the TTPCA SharePoint folder.

Personal details of prisoners should not be removed from a prison site.

Destruction of personal information about prisoners

All personal information that specifically identifies prisoners (first name, last name and PRN number) will be automatically deleted in ā-kanohi referral management tool 15 months after it has been entered.

Any physical notes that chaplains take about prisoners while providing pastoral care is considered personal information if they identify prisoners in any way. These physical records are destroyed after 15 months. Chaplains at each prison site are responsible for ensuring that

physical records are destroyed within this timeframe. Secure destruction of information can be completed by putting the records into secure paper bins or using a shredder at the prison site.

Where information has been recorded about prisoner behaviour incidents, for safety reasons this information will be held until such time as the prisoner is no longer held on site.

Use of prisoners' personal information

Prisoners' personal information is used so that TTPCA can report to its stakeholders on the services that have been provided. TTPCA's reports to internal and external stakeholders will highlight trends and demographics but these reports will not identify individual prisoners.

TTPCA also uses personal information to review and improve its services to all prisoners and follow up any problems or issues that prisoners may have.

Chaplains will use personal information about prisoners, such as names, for the purposes of contacting and scheduling requested meetings with them.

Information about prisoner behaviour incidents is used for the purpose of ensuring these incidents are appropriately managed by Corrections/Serco staff. TTPCA staff at the prison site also retain this information for the purpose of adopting appropriate safeguards to ensure the ongoing safety for chaplains and volunteers.

TTPCA will use the personal information obtained from prisoners as part of a TTPCA investigation for the purposes of carrying out an investigation and assessment of a complaint.

Personal information obtained about prisoners cannot be used for any other purpose than the purpose for which it was collected, except with the prisoner's express consent or where there is a legal requirement or a safety requirement to disclose that information (see Disclosure of personal information section below).

Disclosure of prisoners' personal information

In some circumstances prisoner information may be shared either internally or externally. In each of those circumstances certain conditions will need to be met to permit the sharing of information.

The following are circumstances where information can be shared:

Sharing of information within TTPCA

Chaplains will not share prisoner names and/or details in reports, emails and verbal conversations with staff and volunteers in TTPCA, unless those details are required for the other person to undertake their role.

Sharing of information with Corrections or partner agencies

Prison staff can only see records of prisoner attendance at group services and records of when a prisoner meets a chaplain, if they have the prisoner's permission.

There may be rare occasions where chaplains need to share a prisoner's personal information with Corrections for their or someone else's safety, or where it is necessary to uphold the law.

Staff may use personal information to alert Corrections or Serco to an incident of prisoner misconduct. Staff may also use personal information to raise concerns with Corrections or Serco about actual or threatened harm to a person or people. In this situation, critical information relating to a prisoner's safety will be passed on to Corrections staff for entry into their Integrated Offender Management System (IOMS). For example, this might be when a prisoner talks about suicidal ideation or provides information relating to someone else's safety.

Staff and volunteers should refer to the Reports of Concern policy for more detailed guidance on how to manage personal information if they have concerns about actual or threatened harm to a person or people.

While establishing and maintaining trust with prisoners is important, chaplains will need to manage discussions with prisoners to alert them to reporting requirements when there is a concern about someone's safety.

Prisoners do not need to consent to information about them being provided to Corrections and Serco as part of quarterly reports if they cannot be identified from that information.

Personal information of a prisoner will not be shared with partner agencies (i.e. agencies supporting prisoners with their rehabilitation or the reintegration process into the community) unless the prisoner has provided express written permission, or when there is a legal requirement for this to occur.

Sharing of information by Corrections to TTPCA

Prisoners are advised in the *Spiritual support in prison* brochure that chaplains can access prisoner information if they have a proper reason to do so. For the purpose of undertaking one-on-one sessions requested by a prisoner, chaplains may obtain limited personal information from Corrections where it is relevant to the delivery of chaplaincy. This may include, for example, the chaplain's use of IOMs or Booking Tool (Corrections systems) to access prisoner location and safety alerts of a prisoner who has requested a pastoral care session with the chaplain. The chaplain will use this information solely for the purpose of organising a pastoral care session with the prisoner.

In addition, prisoners often ask a Corrections officer staff to see a chaplain. In such a situation, Corrections can provide a prisoner's name, location and their request for pastoral care to the chaplain. This personal information is shared on the basis that the prisoner has authorised this disclosure by making the request to see a chaplain.

Sharing of information with external parties

Ideally chaplaincy supported communication between outside parties and prisoners should be limited to activity specifically concerned with pastoral care events (e.g., grief situations - funerals). In these cases, communication with external parties requires the approval of prison staff. All other types of communication should be done by prison staff.

When contacted by a member of the public (e.g. a family member requesting that a chaplain visit a prisoner), the chaplain (or other staff member or volunteer) will not confirm whether or not the prisoner is, in fact, at the prison. The staff member or volunteer can direct the inquirer to the Corrections website which has a form for making these requests.

Sharing information in a court process

Communication between a prisoner and a chaplain is privileged when it occurs within the capacity of a chaplain carrying out their duties. In relation to a court proceeding, a chaplain has the right not to disclose any privileged information. The Evidence Act 2006 (sections 53 and 58) covers this provision. It is worth noting that while a chaplain can exercise privilege in relation to a request or demand for private information, the chaplain should consider whether withholding the information would significantly harm the public interest. In all cases the chaplain should raise these types of situations with their manager.

Sharing information with the Police

A chaplain may hear a prisoner admit to crime that has not come to the attention of the Police. In these circumstances a chaplain cannot disclose to the Police or other agency details about the crime or the prisoner who committed it. Under the Privacy Act the chaplain only receives information for the purposes of pastoral care, and so information received about a crime cannot be used for another purpose, such as law enforcement, without the prisoner's permission. The exception is where there is threat to personal safety or where a previous incident of abuse is divulged in relation to a child or young person. Where these scenarios occur, the chaplain should follow the reporting requirements of the Report of Concern policy.

Consent for the publication of prisoner information

Staff should obtain prisoners' consent in writing before publishing personal information (i.e., as case studies or a story) about them in any external TTPCA publication such as the TTPCA annual report. Anybody can withdraw their consent for this at any time before the report is published. Anybody who is featured in a case study or story in the annual report or a similar publication should be informed of how the report will be publicised and distributed and be offered a copy (where appropriate) when it has been published.

Volunteers

Collection of volunteers' information

TTPCA collects volunteer information for three main purposes:

1. To help TTPCA assess a volunteer application in relation to volunteer opportunities that TTPCA may have available. Prospective volunteers will need to submit pertinent personal information as part of their application. TTPCA will only ask for personal information relevant to applicants' suitability for undertaking the volunteer role.

Prospective volunteers will also need to give consent for their personal information to be collected by TTPCA from third parties – this includes, for example, references and their criminal conviction history.

2. To help TTPCA maintain contact with volunteers and any next of kin (for emergency purposes)

3. To help TTPCA manage incidents, conduct and performance issues around a volunteer's activity

Note: Staff should make volunteers aware when this information is being collected and seek their permission where this is necessary.

Storage of volunteers' personal information

Any personal information about volunteers which identifies them is saved into Better Impact (TTPCA's secure volunteer management database) and in TTPCA's Microsoft Office 365 programmes. For example, some information about volunteers may be kept in TTPCA's SharePoint when it concerns incidents, behaviour and performance.

All information will only be retained for as long as that information is needed for the purpose of volunteering.

Where an individual ceases to be a volunteer, TTPCA will archive their personal information for a period of two years. After two years, all information about the archived volunteer will be

deleted, except for the volunteer's name, date of birth, period of service and the reason for them ceasing their volunteer work with TTPCA. Where a volunteer has been dismissed from TTPCA, a summary of the details of their dismissal will also be retained.

Use of volunteers' personal information

Personal information of prospective and existing volunteers is used for the following purposes:

1. Determining suitability in relation to volunteer opportunities that TTPCA may have available.
2. Manage a volunteer's ongoing participation in volunteering. For example, criminal history clearances (and renewals) and other personal details that are pertinent to a volunteers ongoing suitability are retained as a basis of determination of suitability for current and future TTPCA volunteer roles. This information may also be accessed to assist the investigation and management of any problems or issues that involve a volunteer. In addition, volunteers' contact details are used to ensure ongoing communication from TTPCA to volunteers about scheduling of volunteer sessions or training and for the distribution of newsletters.

Information on volunteers cannot be used for any other purpose than the purpose for which it was collected, except with the volunteer's express consent or where there is a legal or safety reason to disclose the information (see Disclosure of personal information section below).

Disclosure of volunteers' personal information

Safeguarding of volunteers' personal information within prisons is critical. Volunteers should only reveal their first names to prisoners and no details of an individual's private life or personal details are to be discussed within the prison environment.

Personal information held by TTPCA about a volunteer will not be disclosed unless the volunteer provides authorised consent for this to occur. The exception is those rare occasions where disclosure is necessary to avoid endangering someone's health or safety, or, where disclosure is granted by law.

Staff and prospective staff

TTPCA collects information from staff during two periods of activity, at the time of recruitment and during their employment.

Note: TTPCA should make staff aware when information is being collected and seek their permission to use it where this is necessary.

Collection of personal information during staff recruitment

When recruiting for a vacant role, TTPCA will only ask for information that is relevant to an applicant's suitability for the role. Therefore, recruitment panels are required to use the following practices in the recruitment process:

- Applicants' identities are kept confidential to those who are directly involved in the recruitment process.
- Applicants need to give their express consent for their personal information to be collected from third parties, including references, drug testing and their criminal conviction history.
- References are only sought from the people the applicant has nominated as their referee. Applicants must consent should any other person be sought as a referee. The person conducting the referee check will confirm with the referee if they wish to have their

comments about the applicant kept confidential, otherwise there may be an obligation to disclose details if the applicant were to request this.

Collection of personal information from staff during employment

On occasion, personal information may be collected from a staff member during the course of their employment for the purpose of TTPCA managing the staff member's activity. This may occur when:

- requesting updated emergency contact information from staff members or updated IDs as part of the Ministry of Justice criminal check process
- generating information as part of salary reviews and performance reviews
- the staff member is having their performance or conduct managed
- gathering information for publicity activity (for example, use on the TTPCA website or in the annual report)

Storage of personal information during recruitment

To help TTPCA assess an application for vacant roles, candidates will need to submit pertinent personal information. In order to prevent unauthorised access, this information will be stored securely – both electronically in password protected folders and for hard copy records, in locked filing cabinets.

The applications of unsuccessful candidates will be securely destroyed unless the candidates have given their consent for their information to be kept on file in case another suitable vacancy opens in the future. Electronic files will be deleted from the system and secure destruction of hard copy information will involve putting records into a secure paper bin or using a shredder.

If a recruitment agency is engaged for the recruitment process on TTPCA's behalf, TTPCA is responsible for ensuring the agency meet all privacy obligations to applicants.

Storage of personal information about staff during employment

A record of interview notes, referee checks and identification will be retained on electronic personnel files for all new staff employed at TTPCA. In addition, all other relevant personal information will be held securely on electronic personnel files and in customised systems, for example, the payroll system.

Following an employee finishing their employment with TTPCA, personnel files must be kept for at least six years, and PAYE records must be kept for seven years. Both types of records are subject to withholding grounds but can be made available on request to staff members' union or other representative(s) or Labour Inspectors and Immigration Officers. Documents will be securely destroyed (shredded or deleted) when they are due for destruction.

Use of personal information during recruitment and employment

Information obtained in a recruitment process cannot be used for any other purpose than deciding on a candidate's employment application or if there is a subsequent review of the recruitment process, except with the applicant's express written consent.

Personal information about existing staff will only be used by TTPCA for the express purpose for which it has been collected, largely to enable the management of a staff member's employment in line with legislative and best practice HR requirements. Information on staff cannot be used for any other purpose than the purpose for which it was collected, except with

the staff member's express consent or where there is an obligation to disclose the information (see Disclosure of personal information section below).

Disclosure of personal information during recruitment and employment

During recruitment, panel members will not breach any applicant's privacy by doing anything that might reveal the applicant has applied for the role. This applies to the location of the interview and who may be spoken to about their application. Discretion is critical when making any arrangements related to recruitment.

Personal information of a staff member will not be disclosed to third parties unless the staff member provides authorised consent for this to occur. The exception is in those rare occasions where disclosure is necessary to avoid endangering someone's health or safety, or, where disclosure is granted by law.

Requests to access or correct personal information

Procedure for responding to requests to access or correct personal information

On occasion, a prisoner, staff member, volunteer, contractor (or any other party who has had some engagement with TTPCA) may request to access personal information that is held by TTPCA about them. Prisoners and volunteers can make an initial request to a chaplain. Staff members can contact their manager or the Senior HR Advisor in the first instance. A request does not need to be in writing, however best practice is to ask for the request to be made in writing. Once a request has been made, the following process is undertaken:

1. All requests to access or correct information will be referred to the Privacy Officer for consideration.
2. Requests to access or correct information will be considered positively and TTPCA will aim to respond to such requests as soon as possible but no later than 20 working days after receiving the request.
3. If TTPCA does not hold the information that a person has asked to be corrected and believes that another agency holds it (like Corrections), TTPCA will transfer the request to that agency within 10 working days of receiving it and inform the person who made the request accordingly.
4. If a decision is made by the Privacy Officer to refuse access or to correct personal information (partially or fully), the Privacy Officer will explain why this decision was made following the provisions of the Privacy Act.
5. If a request to correct information is refused, the requester can make a statement of correction that TTPCA will attach to all available copies of the documents and/or information that the person asked to be corrected.
6. If a request to access or correct information is accepted, the access will be given, or the correction made, as soon as reasonably possible.

Handling breaches of privacy and complaints

Privacy breaches

A privacy breach is the unauthorised or accidental access to someone's personal information or disclosure, alteration, loss, or destruction of personal information.

TTPCA will act quickly and transparently with all relevant parties when a potential or actual breach is identified.

Procedure for assessing harm from privacy breaches

1. If TTPCA staff or volunteers become aware of a potential privacy breach, they will inform the Privacy Officer as soon as possible.
2. The Privacy Officer, together with any relevant staff member involved with the potential breach, will consider any steps that can be taken immediately to limit the potential breach or limit harm from the potential breach.
3. The Privacy Officer will complete the *Privacy Breach incident form* (see Appendix 2) and will use the Privacy Commissioner's online self-assessment tool, *NotifyUs*, as a guide to help determine whether a privacy breach is likely to cause serious harm.
4. Whether harm is "serious harm" depends on the circumstances of the privacy breach. Some questions to consider when assessing whether a breach is likely to cause serious harm include:
 - how sensitive is the information that is involved in the breach?
 - who has obtained or may obtain the information?
 - what types of harm may be caused to people affected by the breach?
 - how likely is it that someone will be harmed because of the breach?
 - what steps have been taken to reduce the risk of harm or further harm from this breach?
 - are there security measures in place that protect the information from being accessed?
 - is someone's physical or psychological safety in immediate danger?
 - is someone at risk of serious financial harm?
5. If the Privacy Officer assesses that a privacy breach is likely to cause serious harm, they will notify the Office of the Privacy Commissioner and all affected parties as soon as possible (and no later than 72 hours after TTPCA became aware of the breach). They will also inform the Chair of the Board.
6. After the breach is resolved, TTPCA will review whether the breach was due to a systematic problem or was an isolated event and will take any fair and necessary steps to strengthen security procedures for future privacy protection.

Privacy Complaints

The Privacy Officer will be responsible for dealing with complaints alleging a breach of the Privacy Act. The Privacy Officer will facilitate the fair, simple, and efficient resolution of complaints.

Procedure for handling complaints

1. Any complaints from prisoners, volunteers, or staff that allege a privacy breach should be made or referred to the Privacy Officer.

2. The Privacy Officer will:

- acknowledge the complaint in writing within 5 working days of receipt.
- inform the complainant of the relevant internal and external complaints procedures
- document the complaint and the actions taken to respond to the complaint.

3. Within 10 working days of acknowledging the complaint, TTPCA will decide whether it accepts that the complaint is justified or not.

4. If TTPCA decides that more time is needed to investigate the complaint, it will:

- determine how much additional time is needed
- if that additional time is more than 20 working days, inform the complainant of that determination and of the reasons for it.

5. As soon as practicable after TTPCA decides to accept that a complaint is justified or not, the Privacy Officer will inform the complainant of:

- the reasons for the decision
- any actions TTPCA proposes to take
- the right to complain to the Privacy Commissioner.

Appendix 1: Security Measures to Safeguard Personal Information

To support the privacy of all personal information, TTPCA adopts the following safety measures with regards to paper-based and electronic personal information. Further information about the IT measures used to protect prisoners, staff and volunteer data can be found in the TTPCA Information Technology Policy.

Security of Paper Based Documentation

All paper-based (hard copy) personal information is kept in secure filing cabinets.

Paper based documentation such as employee personnel files, recruitment files and payroll records are kept in accordance with appropriate retention periods in a secure location at National Office.

Any personal records relating to prisoners are held securely in locked cabinets on-site at prisons.

Protection of Electronic Data from unauthorised access

Oversight of TTPCA's IT security

TTPCA takes the security of its IT systems seriously and has implemented measures to safeguard against unauthorised access, theft, and other threats.

The oversight of all TTPCA's IT security measures is provided by an external IT company (Mercury IT) who provide the necessary specialist and expert knowledge that is beyond TTPCA technical capability.

TTPCA complies with all applicable laws and regulations related to IT security, including those set by the Department of Corrections.

Staff training, induction and responsibilities

All employees must comply with TTPCA's IT security policies, including the use of strong passwords and two-factor authentication where appropriate, regular software updates, and reporting of any security incidents. In addition, all TTPCA users are required to undertake training in IT security at the commencement of their employment and as required for their role.

Corrections and Serco also provide information to site staff on best IT practice during the course of their employment.

Firewalls

TTPCA and Mercury IT has implemented an enterprise class (Mikrotik) firewall which provides industry standard firewall security and managed access to the network. TTPCA actively monitors malware threats, unusual activity reports and unusual login attempts.

Antivirus Software

TTPCA and Mercury IT ensures that appropriate software to protect against viruses is installed. All computers (and devices running Business Premium licenses) have the Microsoft Defender ATP anti-virus and anti-malware software installed, running and monitored. The software is automatically updated as and when new updates are available from Microsoft and are checked during our operational maintenance.

Access Control

All employees only have access to systems which are required for them to undertake their roles. Access to sensitive data and IT systems is restricted to authorized personnel only.

All employees have access to SharePoint, and only to areas which are necessary for them to undertake their role(s). Personal information in Better Impact (the TTPCA volunteer database), ā-kanohi referral management tool and Department of Corrections systems can only be accessed by the people who are authorised to do so. The systems are protected by multi-step authentication and/or passwords where that is available. Other systems with personal information (including the payroll system) are also only accessible by those authorised to do so.

Password protection

TTPCA adopts best practice in relation to password management guidelines.

All staff are required to set strong and unique passwords. As a rule, passwords should:

- 1) Be used for one account only, not reused across many accounts
- 2) Not be based on personal information that could be found online
- 3) Be long and strong, such as a passphrase made up of four or more words
- 4) Be kept safe and not written down.

TTPCA has set up restrictions to prohibit vulnerable passwords such as Password! Or Welcome1. TTPCA also has settings that enforce password restrictions, and password change and reset history.

In line with best practice, there is no default expiration value for passwords. Staff should only have to change their password if they suspect that their account, or the TTPCA network, might be compromised in some way.

Staff are encouraged to use two-factor authentication where that is possible to add a layer of security to accounts.

Regular review of systems

TTPCA has processes to ensure that access to systems remains available only to those who are authorised to use them. Checklists for new starters and exited employees ensure that only current employees have access to the systems. TTPCA also conducts regular reviews of system access, including a monthly review of user access to ā-kanohi referral management tool, to ensure that systems are only accessed by the appropriate people.

Physical security of IT hardware and devices

TTPCA recognises the importance of IT asset management. Therefore, TTPCA maintains accurate inventory records, which maximises the use of existing assets, and minimises the risk of unauthorised access or theft.

TTPCA maintains an up-to-date inventory of all IT assets, including hardware, software, and other technology resources.

E-waste disposal

TTPCA ensures that all technology items are disposed of in an ethical, environmental, and secure manner. TTPCA follows a checklist to ensure that the disposal of e-waste is undertaken in an appropriate manner. Computers and phones, for example that can no longer be used are disposed of by an e-waste process that ensures that any sensitive data residing on the electronic item is deleted and can no longer be accessed.

Appendix 2: Privacy Breach Incident Form

Privacy Breach Incident Form

For completion by TTPCA Privacy Officer (or delegated officer)

Date of Notification:

Reported by:

Date the breach occurred:

Name(s) of staff member(s)/volunteer involved in breach:

Location of the breach:

Description of Incident

Provide a description of the incident including:

- the type of personal information involved in the breach,
- how the breach occurred,
- who was affected/ how many individuals were affected, and
- steps already taken to contain the breach and/or reduce harm.

Assessment of Privacy Breach

Use the below table to assess whether the breach is likely to cause serious harm to the affected individual(s):

In weighing up the likelihood of serious harm consider the sensitivity or significance of the information lost and the possible intentions of the recipient.

Serious Harm category:	Please select rating:			Notes:
Likelihood of serious harm to the affected individual from financial fraud	Low	Medium	High	
Likelihood of serious emotional, reputational or psychological harm to the affected individual	Low	Medium	High	
Likelihood of blackmail occurring towards to the affected individual	Low	Medium	High	
Likelihood of serious physical harm or intimidation to the affected individual	Low	Medium	High	
Likelihood of harm to the affected individual due to identity theft	Low	Medium	High	

Serious Harm category:	Please select rating:	Notes:
Likelihood of employment harm to the affected individual	Low Medium High	

Based on the above table, is the breach likely to cause serious harm? Yes/No

If yes, the Office of the Privacy Commissioner and affected individual(s) must be notified.

Date of notification to Office of the Privacy Commissioner:

Date of notification to affected individual(s):

If the breach is not likely to cause serious harm, should the affected individual(s) be notified?

Yes/No (Please provide reason for decision):

If yes, date of notification to the affected individual:

Current Status of Breach

Has the breach been contained? Yes/ No

If yes, describe actions taken:

If no, describe what further steps are needed:

Follow Up Actions

Assessment of the cause of the breach (please select):

- Human error
- IT / systems error
- Appropriate security settings not being appropriately applied
- Malicious action (by volunteer or staff member)
- Malicious action (by external party)
- Other, please describe:

If human error or malicious action, is a potential TTPCA misconduct investigation (staff or volunteer) being conducted? Yes/No (Please provide reason for decision)

Describe any recommended follow-up action. This may include policy updates, staff training, system security improvements, etc.

Privacy Officer details

(name)

(title)

T: XX XXXX

Approved by: John Axcell
Date approved: 19 December 2025
Review date: December 2027

E: x.x@prisonchaplaincy.org.nz

Copies to: XXX

To be filed in Privacy Incident Register.