Privacy Policy for CadetNet

Almost any organisation that holds personal information is required to comply with the Privacy Act. This includes the New Zealand Cadet Forces (NZCF). This is the public-facing Privacy Statement that individuals will be required to agree to as a condition of membership. It includes privacy information for all NZCF personnel, split into a ready reference poster from the Office of the Privacy Commissioner and a detailed breakdown of the principles and their application to the NZCF.

Privacy Statement

The following brief statement is included in the NZCF 2A, CadetNet sign-up and other enrolment documentation collecting personal information.

New Zealand Cadet Forces' Privacy Statement

We need certain personal information from you in order to operate. You must agree to us having this information to join NZCF. In collecting and storing this information, we are bound to look after it as per the Privacy Act 2020.

Information we collect includes:

Information we collect includes:	We need this so:
Basic information about you such as your full name, date of birth, gender and school	We can identify you.
Your service history with the NZCF	We can manage your progression through the organisation and manage issues that are ongoing, disciplinary, or otherwise.
Your National Student Number	We can award any credits you earn through NZCF.
Your address and contact details	We can contact you and return you home in an emergency.
Address and contact details for your primary caregiver and an alternative next of kin.	We can contact your parent or caregiver, or a next of kin in an emergency or we require parent/caregiver permission for you to attend an activity. Also, to provide to the Unit Support Committee (USC) so they can manage any fees or costs incurred for Unit activities.
Any dietary requirements.	We can ensure you get the food you need.
Illnesses or medical conditions you are suffering from, and medication that you are taking.	We can effectively manage risk on activities by ensuring we do not endanger you or anyone else. In the event of a medical emergency, we can give responders all necessary info.
Your bank account details, tax code and IRD number.	We can pay you (only collected if you staff a paid Authorised Activity).

This information can be stored in personal files which are secured by lock, on permission slips for activities which will be kept by responsible officers and destroyed afterwards, and on the CadetNet database which uses reasonable electronic security. The last five items are treated as **"staff-in-confidence"**, which means extra care is taken in keeping the information confidential. We will only disclose that information to NZCF staff (Officers, Officer Cadets and Supplementary Staff) who work at your unit, headquarters or on an activity you are attending and Next of Kin information to the USC so they can manage the Unit finances.

You may request to see, and correct personal information held about you at any time. Once you leave, the NZCF undertakes to destroy any personal information about you within three years. The NZCF will not disclose this information to third parties unless we have a good reason (such as a medical emergency).

Basics of the 13 Privacy Principles

A quick tour of the privacy principles

The Privacy Act 2020 has 13 privacy principles that govern how you should collect, handle and use personal information.

1 You can only collect personal information if it is for a lawful purpose and the information is necessary for that purpose. You should not require identifying information if it is not necessary for your purpose.

2 You should generally collect personal information directly from the person it is about. Because that won't always be possible, you can collect it from other people in certain situations. For instance, if:

- the person concerned gives you permission
- collecting it in another way would not prejudice the person's interests
- collecting the information from the person directly would undermine the purpose of collection
- you are getting it from a publicly available source

3 When you collect personal information, you must take reasonable steps to make sure that the person knows:

- why it's being collected
- who will receive it
- whether giving it is compulsory or voluntary
- what will happen if they don't give you the information

Sometimes there may be good reasons for not letting a person know you are collecting their information – for example, if it would undermine the purpose of the collection, or if it's just not possible to tell them.

4 You may only collect personal information in ways that are lawful, fair and not unreasonably intrusive. Take particular care when collecting personal information from children and young people.

5 You must make sure that there are reasonable security safeguards in place to prevent loss, misuse or disclosure of personal information. This includes limits on employee browsing of other people's information.

6 People have a right to ask you for access to their personal information. In most cases you have to promptly give them their information. Sometimes you may have good reasons to refuse access. For example, if releasing the information could:

- endanger someone's safety
- create a significant likelihood of serious harassment
- prevent the detection or investigation of a crime
- breach someone else's privacy

7 A person has a right to ask an organisation or business to correct their information if they think it is wrong. Even if you don't agree that it needs correcting, you must take reasonable steps to attach a statement of correction to the information to show the person's view.

8 Before using or disclosing personal information, you must take reasonable steps to check it is accurate, complete, relevant, up to date and not misleading.

9 You must not keep personal information for longer than is necessary.

10 You can generally only use personal information for the purpose you collected it. You may use it in ways that are directly related to the original purpose, or you may use it another way if the person gives you permission, or in other limited circumstances.

11 You may only disclose personal information in limited circumstances. For example, if:

- disclosure is one of the purposes for which you got the information
- the person concerned authorised the disclosure
- the information will be used in an anonymous way
- disclosure is necessary to avoid endangering someone's health or safety
- disclosure is necessary to avoid a prejudice to the maintenance of the law

12 You can only send personal information to someone overseas if the information will be adequately protected. For example:

- the receiving person is subject to the New Zealand Privacy Act because they do business in New Zealand
- the information is going to a place with comparable privacy safeguards to New Zealand
- the receiving person has agreed to adequately protect the information – through model contract clauses, etc.

If there aren't adequate protections in place, you can only send personal information overseas if the individual concerned gives you express permission, unless the purpose is to uphold or enforce the law or to avoid endangering someone's health or safety.

13 A unique identifier is a number or code that identifies a person in your dealings with them, such as an IRD or driver's licence number. You can only assign your own unique identifier to individuals where it is necessary for operational functions. Generally, you may not assign the same identifier as used by another organisation. If you assign a unique identifier to people, you must make sure that the risk of misuse (such as identity theft) is minimised.

Breakdown of NZCF Privacy Obligations

The New Zealand Cadet Forces ("NZCF") is defined as an agency (being "any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector") within the Privacy Act 2020 ("the Act"). Consequently, the NZCF is bound by the information privacy principles outlined in Part 3 of the Act. This breakdown outlines the principles and how the NZCF can ensure it complies with them.

Any questions or concerns about your privacy obligations as a staff member of NZCF can be directed to the Executive Officer of the NZCF who acts as the organisation's Privacy Officer, advising on compliance with obligations under the Act.

The Information Privacy Principles

Part 3 of the Act contains the 13 Privacy Principles with which compliance is required.

Principle 1

Principle 1 requires that personal information shall not be collected unless for a lawful purpose connected with a function or activity of the agency, and that the collection of the information be necessary for that purpose.

The NZCF collects personally identifiable information comprised of cadets' full name, date of birth, gender, contact details (phone number, email address, residence address), medical conditions, educational institution, employer, next of kin/guardian details (name, contact details, relationship with the cadet, employer), swimming ability, involvement in sports and other organisations and service history with the NZCF.

This information is collected for the purpose of the individual's membership in the NZCF. Officers of the NZCF (and to a lesser extent, NZDF staff posted to NZCF) are bound under the Care of Children Act 2004 and other relevant legislation, as well as the common law doctrine of in loco parentis (commonly applied to teachers), with a legal duty of care over the individual as most are under the age of 18, and need access to this information in order to execute this duty.

Medical information is traditionally regarded as being at the high end of the spectrum in terms of confidentiality, but disclosure is necessitated by this legal duty and the adventurous, higher-risk nature of some of the activities carried out by NZCF (e.g. tramping, gliding, sailing, target shooting).

Contact details of the individual are necessary to keep them informed about NZCF activities, and of the next of kin/guardian both for provision of said information and fulfilment of the legal duty (for example, an NZCF officer may need to contact a cadet's next of kin/guardian in the event of a medical incident). Next of kin/guardian information may be passed to the USC Branch and the respective Association solely for the purpose of financial management of the Unit e.g. collecting activity fees.

Involvement in sports and other organisations and service history with the NZCF (including course performance reports and other internally-generated documents) are collected for the purpose of managing the individual's involvement and progression in the NZCF.

Principle 2

Principle 2 requires that personal information be collected directly from the individual concerned.

The information is sourced directly from the individual upon their application for membership in the NZCF in the application form (electronic or hard copy). Where certain information such as internally generated documents (course performance reports) is not sourced directly from the individual concerned, or is supplied by one NZCF officer to another (or NZDF staff posted to NZCF), it falls under the exceptions in paragraphs (b) and (c), as it is a condition of membership that the individual authorises sharing of the information within NZCF between NZCF officers (and with NZDF staff posted to NZCF), and the generation and sharing of course reports with the same, and this does not prejudice the interests of the individual concerned.

Principle 3

Principle 3 requires that the NZCF take a number of steps that are reasonable in the circumstances when collecting the personal information directly from the individual.

Upon application, individuals are required to fill out the aforementioned 'Cadet Enrolment Form – NZCF2' (or electronic equivalent). At the time, they are informed of necessary details, through the privacy policy statement on the CadetNet site or in person by the NZCF officer providing the form. These details include the purpose of collection (stated under Principle 1 above), intended recipients as NZCF officers and Next of Kin information for the USC, an overview of the NZCF as the collecting and holding agency and the address of their unit as the local branch, the consequences of refusal to provide (membership is conditional upon provision), and that they have the right to view and request correction of that personal information. This privacy policy statement remains available to read on the CadetNet site at any time.

Principle 4

Principle 4 requires that information is not collected by unlawful means or in circumstances that are unfair or intrude to an unreasonable extent upon the personal affairs of the individual concerned. Particular care is to be taken when collecting personal information from children and young people.

The NZCF has taken steps to ensure that it and its agents (NZCF Officers and NZDF Staff posted to the NZCF) collect personal information in accordance with its legal obligations under the Privacy Act 2020, including the provision of this privacy policy statement on the CadetNet site. All collection of information is upfront and in good faith, and all information requested is justifiable for the purposes of the individual's membership in the NZCF.

Principle 5

Principle 5 requires that the information is protected by security safeguards that are reasonable in the circumstances against loss; unauthorised access, use, modification or disclosure; other misuse; and that when providing it to a person in connection with the provision of a service to the NZCF, everything reasonably within the power of the NZCF is done to prevent unauthorised use or unauthorised disclosure of the information.

The NZCF has robust policies to ensure the security and avoidance of unauthorised disclosure of personal information. All NZCF Officers and NZDF Staff posted to the NZCF are authorised to access the held personal information of any member of the NZCF as a condition of membership of the NZCF. Furthermore, members of the NZCF holding the rank of Officer Cadet or are Supplementary Staff and hold a current security clearance and relevant administrative appointment in the individual's unit are also authorised to access their personal information. This is disclosed to the individual upon application to join the NZCF as detailed above. Personal information is classified as **"Staff-in-Confidence"** which is recorded upon any documentation containing it or electronic equivalent, and as a matter of policy only the authorised personnel listed above, and the individual concerned may view such documentation or electronic record.

Documentation is required to be stored in filing cabinets within secured (lockable) offices. Information stored on the CadetNet site is only accessible by the authorised personnel and the individual concerned through their individual logins and appropriate electronic security measures (authentication, firewalls, etc.) are used. Other members of the NZCF not being officers, NZDF staff posted to the NZCF, Officer Cadets or Supplementary Staff not holding a relevant administrative appointment in the individual's unit are prohibited from accessing **"Staff-in-Confidence"** information and any contravention is regarded as a serious breach and dealt with through an appropriate disciplinary procedure. The security safeguards around the storage of such information and good supervision by NZCF officers prevents such breaches.

Principle 6

Principle 6 requires that readily retrievable information is available to the individual on request. When such a request is made, the individual must be advised that they may request correction of it.

NZCF units should seek to update personal files at least annually in consultation with individuals. It is strongly recommended that permission slips incorporating a medical disclosure be required for all planned activities outside of parade nights (NZCF 8s or variants of), so that up to date medical information is obtained and can be checked against any information already held. These permission slips should be destroyed as soon as practicable after the activity.

Individuals should be reminded that they may request to see and/or correct personal information at any time, and where such a request is made, it should be accommodated as soon as practicable.

Principle 7

Principle 7 requires that individuals can request correction of any held personal information to ensure it is accurate, up to date, complete, and not misleading.

NZCF units should seek to update personal files at least annually in consultation with individuals and incorporate permission slips including medical disclosures for activities outside of parade nights (NZCF8s or variant), as detailed above. Checking them against any information already held also gives individuals an opportunity to correct personal information.

Principle 8

Principle 8 requires that steps, that are reasonable in the circumstances, are taken to ensure that information used is accurate, up to date, complete, relevant, and not misleading.

NZCF units should seek to update personal files at least annually in consultation with individuals and incorporate permission slips including medical disclosures for activities outside of parade nights (NZCF 8s or variant), as detailed above.

Checking them against any information already held also gives individuals an opportunity to correct personal information.

Principle 9

Principle 9 requires that personal information not be kept for longer than is required for the purposes for which it may lawfully be used.

As stated above, the information is generally collected for the purpose of the individual's membership in the NZCF. Termination of an individual's membership in the NZCF will therefore have the effect of terminating that lawful purpose. On release, the NZCF archives the electronic information held in CadetNet and only non-identifiable information is used for statistical purposes. An individual's personal electronic information is no longer available to their former Unit, their Area Office or Headquarters NZCF.

Units holding hard copy personal information are to return it to the owner on their release. If the return of the information is not possible it is to be retained for no longer than one year allowing them access to records (e.g. course reports) for CV/career reasons – after which NZCF units must destroy it (preferably by shredding).

HQNZCF operate a procedure whereby certain personal information relating to an individual's career and achievements in the NZCF are retained beyond this window in a quarantined digital space only accessible by a restricted category of staff for the purpose of supplying CV-supporting info to former cadets or easily re-enrolling returning cadets as staff.

Principle 10

Principle 10 requires that personal information is used for the purpose for which it was obtained, unless there is a valid reason for doing otherwise. This can include the information being publicly available, such use being authorised by the individual, such use being required by law, or the information being anonymised such that the individual is not identifiable.

NZCF units must ensure they implement robust procedures to ensure personal information they hold is not accessible by unauthorised personnel or used for any other purpose than genuinely that detailed under Principle 1.

This includes:

- Enforcement of Staff-in-Confidence restrictions on all medical disclosures, contact details, course reports and personal files (including disciplinary or performance management information);
- Policies restricting access to said personal information to staff members who have a bona fide reason e.g. running an activity, staffing a course, involved or consulting on a disciplinary investigation, unit staff; and
- Providing next of kin information to the USC for the sole purpose of financial management of the Unit e.g. collecting activity fees.

Principle 11

Principle 11 requires that personal information is not disclosed unless permitted on certain grounds, as detailed above in principle 10.

NZCF units must ensure they implement robust procedures to ensure personal information they hold is not accessible by unauthorised personnel or used for any other purpose than genuinely that detailed under Principle 1.

If NZCF staff are uncertain as to whether disclosure would be in compliance with privacy obligations, they should refer up the chain of command to the NZCF Privacy Officer (Executive Officer).

Principle 12

Principle 12 requires that you can only send personal information to someone overseas if the information will be adequately protected. For example:

- the receiving person is subject to the New Zealand Privacy Act because they do business in New Zealand.
- the information is going to a place with comparable privacy safeguards to New Zealand.
- the receiving person has agreed to adequately protect the information – through model contract clauses, etc.

If there aren't adequate protections in place, you can only send personal information overseas if the individual concerned gives you express permission, unless the purpose is to uphold or enforce the law or to avoid endangering someone's health or safety.

The NZCF will not send personal information overseas without the express permission of the individual concerned.

Principle 13

Principle 13 requires that unique identifiers (an identifier other than the individual's name, assigned by an agency) aren't assigned to individuals unless necessary to carry out the organisation's function.

NZDF assigns service numbers to individual members of NZCF staffing authorised activities for the purpose of pay and other functions as casual employees. These should be protected as any other personal information.

There is no need for NZCF staff to assign unique identifiers to members, who should only ever be identified by their name and rank.