

Privacy Policy

Policy Owner: Managing Director
Policy Date: 13 Jan 2022
Review Date: 24 September 2024
Version: 1.5

Contents

1. Objective3

2. Privacy Act 2020.....3

3. Principles of Data Privacy.....3

4. Privacy Officer4

5. Disclosing personal information4

6. Protecting and holding personal information.....5

7. Accessing and correcting personal information5

8. Privacy Statement – External5

9. Privacy Statement – Employees.....6

10. CCTV.....7

11. Reference7

1. Objective

The objective of the Privacy Policy is to ensure that Carrfields collects and stores personal information about its customers, suppliers and staff in a strictly confidential manner and only uses such information for the purposes of ongoing business.

In doing so the company also ensures that it complies with the Privacy Act 2020 in all its operations.

2. Privacy Act 2020

The Privacy Act 2020 came into force on 1 December 2020, replacing the Privacy Act 1993.

Carrfields is defined as an Agency under the Privacy Act and as such is required to comply fully with the Act.

Carrfields are committed to complying with all relevant privacy laws and regulations, including the Privacy Act 2020. As part of our commitment to ensuring the protection of personal information, we annually review and update our privacy policy to ensure that it remains current and effective. As part of this review process, we carefully consider any amendments to the Privacy Act 2020 and incorporate any necessary changes into our policy. We encourage our employees and customers to read our privacy policy and contact us with any questions or concerns they may have about our privacy practices.

More information on the Privacy Act can be found on the website of the Privacy Commissioner: www.privacy.org.nz.

3. Principles of Data Privacy

There are 13 principles in the Privacy Act 2020. These principles are listed below, including how they apply to Carrfields.

| Principle | Description |
|-------------------------------|--|
| 1. Purpose for collection | You can only collect personal information if it is for a lawful purpose and the information is necessary for that purpose. |
| 2. Source of information | You should generally collect personal information directly from the person it is about. |
| 3. What to tell an individual | When you collect personal information, you must take reasonable steps to make sure that the person knows: <ul style="list-style-type: none"> • 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 |
| 4. Manner of collection | You may only collect personal information in ways that are lawful, fair and not unreasonably intrusive. |
| 5. Storage and security | 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. Access | 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. |
| 7. Correction | A person has a right to ask an organisation or business to correct their information if they think it is wrong. |
| 8. Accuracy | 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. Retention | You must not keep personal information for longer than is necessary. |
| 10. Use | 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. Disclosure | You may only disclose personal information in limited circumstances. For example, if: <ul style="list-style-type: none"> • 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. Disclosure outside NZ | You can only send personal information to someone overseas if the information will be adequately protected. 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. Unique identifiers | 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. |

4. Privacy Officer

The Act requires that each Agency appoint at least one person who fulfils the role of Privacy Officer. The responsibilities of the Privacy Officer are to:

- be familiar with the privacy principles in the Privacy Act
- work to make sure the organisation complies with the Privacy Act
- deal with any complaints from the organisation's clients about possible privacy breaches
- deal with requests for access to personal information, or correction of personal information
- act as the organisation's liaison with the Office of the Privacy Commissioner.

The **Chief Financial Officer of Carrfields Holdings Group** acts as Carrfields Privacy Officer.

5. Disclosing personal information

The Company may disclose your personal information to:

Any business that supports our services, including any person that hosts, or maintains any supporting IT system or data function, including cloud-based software, storage and/or systems which are associated with the Company’s functions and/or activities; where disclosure is reasonably necessary for the provision of such support.

A credit reference agency to conduct a credit check on you in specific situations, such as when setting credit limits on accounts.

The Ministry of Justice and/or New Zealand Police, or other parties, including former employers for the purposes of pre-employment checks, for example - reference checking;

An agency or other entity that can require us to supply your personal information, for example – the Privacy Commissioner, Government agencies, law enforcement, etc.

Any other person authorised by you, for example – a legal representative or union.

Businesses that support our services and products including some which may be located outside New Zealand.” This may mean your personal information is held and processed outside New Zealand, for example, cloud storage.

Machinery Manufacturers for the purpose of registering your machine and product warranty.

6. Protecting and holding personal information

- 6.1. The Company will take reasonable steps to keep your personal information safe from loss, unauthorised activity/disclosure, or other misuse.
- 6.2. The Act does not stipulate how long personal information should be kept. However, it does state that personal information should not be kept for longer than is required for the purposes for which the information may be lawfully used. Generally, employee records and personnel files will be kept for up to Six (6) years following cessation of employment following which it will be destroyed.

7. Accessing and correcting personal information

- 7.1. Subject to certain grounds for refusal set out in the Act, you have the right to access your personal information about you that the Company holds and to request a correction to your personal information.
- 7.2. Before you exercise these rights under the Act, the Company may require evidence to confirm that you are the individual to whom the personal information relates.
- 7.3. If the Company is of the view that the correction is reasonable and it is reasonably able to change your personal information, it may make the correction. If the Company does not make the correction, it will take reasonable steps to note on the applicable personal information that you requested the correction.
- 7.4. If you want to exercise either of the above rights, email the Company. Your email should provide evidence of who you are and set out the details of your request in writing, for example - the personal information your request relates to, the correction that you are requesting, what outcome you want, etc.
- 7.5. While generally free, the Company reserves the right to charge you reasonable costs of providing you copies of your personal information or correcting that information and will notify of you any corresponding charges before processing your request.

8. Privacy Statement – External

Carrfields’ current Privacy Statement is available on the company website at www.carrfields.co.nz/privacy-security/.

As at the date of this Policy document, the Privacy Statement was as follows (accessed 5th August 2024):

PRIVACY AND SECURITY

Carrfields Limited (Carrfields) take the utmost precautions to protect our staff, Commission Agents, & customers information. Protecting your personal information is very important to us that is why Carrfields apply the most advanced technical measures relating to best e-commerce practice to protect against loss, alteration or unauthorized third party access to customer information.

We use secure servers and Secure Socket Layer (SSL) data transfer for strong encryption for all our customer information. A SSL certificate or “Secure Certificate” is an electronic document that is stored on our website

that allows “Secure Socket Layer” (SSL) communication which is encrypted. This means that any personal data entered on our website cannot be intercepted and read by any unauthorized third party.

The servers on which we collect and store personal information are kept in a secure environment. Any information collected on the Carrfields website will never be disclosed to any third-party under any circumstances – excepting a court order.

COLLECTION OF STATISTICAL INFORMATION

Carrfields may collect statistical information regarding the pages you visit on our site which is non-identifiable. Occasionally we may also conduct a Customer Survey to help us improve our service, enhance customer satisfaction and gather information regarding farming usage, needs and demographics. Any identifiable information is not requested.

If you have any questions about the personal information we collect online please contact us at marketing@carrfields.co.nz

IP ADDRESSES

Customer IP addresses may be used incidentally to help diagnose problems with our server or for administrative purposes. IP addresses are used to gather broad demographic data on customer traffic patterns and site usage. This information is only used internally and assists us in developing our website to improve our customer’s online experience.

COOKIES

Cookies are a small text file that contains information sent by a web server to store on a web browser, so it can be read back when you return to the site.

Cookies are used by many websites on the Internet and are very beneficial in being able to improve the functionality of websites, and the online experience for the user. Cookies cannot carry viruses and cannot install malware on your computer.

If you wish to control or delete cookies on your computer, you can do this in your web browser’s privacy settings. Please note that disabling cookies may diminish your online browsing experience.

For more information on how to change the cookie settings in your browser, [click here](#).

9. Privacy Statement – Employees

Carrfields Individual Employment Agreements (IEA) require employees to comply with the obligations of the Privacy Act (see Section 27 of the IEA).

Carrfields Policy and Procedures Handbook also has a Privacy Statement in relation to the Drug and Alcohol testing (see Policy and Procedures Handbook Section 16 “Drug and Alcohol Policy”). This statement is replicated below (accessed 5th August 2024):

Privacy Act

All information gathered as a result of testing is collected for the purpose of this policy and will be held on your employee file or other nominated Carrfields representative.

Information will be stored in a secure manner. Information held by Carrfields and by the testing provider may be disclosed to persons within Carrfields involved in the implementation of the policy, and/or arranging suitable Health Rehabilitation programmes.

All information returned to Carrfields shall be made available to the employee involved. An Employee shall be entitled to access their results, seek correction where appropriate and uplift information on termination of their employment with Carrfields.

10. CCTV

Closed Circuit Television (CCTV) cameras are installed and operated for one or more of the following purposes:

- Facilitate staff and public safety
- Improve security and deter criminal activity
- Manage traffic movements in particular areas
- Monitor trespass on Carrfields facilities
- Monitor compliance with Council bylaws
- Capture information that could be used to investigate crime, a health and safety situation and/or staff incidents

The CCTV policy has been created to ensure that Carrfields, its employees and contractors comply with good practice, transparency and accountability and in respect of the requirements of the Privacy Act 2020 when operating CCTV cameras. It also outlines the process for managing all access to CCTV data, the delegated authorities of Carrfields staff and Carrfields obligations in regard to CCTV data storage, security and signage.

11 Reference

P024 CCTV Policy