

Privacy Policy

Prepared by People and Culture

November 2022
AGIL-HR-POL-0003



Contents

1. Privacy Policy	3
1.1 What do we use personal or sensitive information for?	3
1.2 What information do we collect?	4
1.3 How personal or sensitive information is collected?	4
1.4 How do we use personal or sensitive information?	5
1.5 Disclosure of personal or sensitive information	5
1.6 Storage and security of personal or sensitive information	6
1.7 Accessing and updating personal or sensitive information	6
1.8 Complaints and further information	7
1.9 Changes of this Privacy Policy	7

Document Control					
Revision	Issue Reason	Date	Prepared	Reviewed	Approved
0		22/11/2022	Claire Thomas	Bianca Taylor	Craig Bloxham

A person using Agilitus Pty Ltd documents or data accepts the risks of:

- using the documents or data in electronic form without requesting and checking them for accuracy against the original hard copy version; and
- using the documents or data for any purpose not agreed to in writing by Agilitus.

1. Privacy Policy

Agilitus Pty Ltd recognises and respects the privacy of all individuals. As an Australian registered company (ABN 94 628 465 056), Agilitus is bound by the Privacy Act 1988 as amended by the Privacy Amendment (Enhancing Privacy Protection Act 2012 (the Act) and the 13 Australian Privacy Principles (APPs) contained within the Act.

This document sets out the Privacy Policy of Agilitus relating to the protection of 'personal or sensitive information' as defined by the Act. All employees, officers and directors of Agilitus are required to comply with this Privacy Policy. Information that can identify an individual (or that can be used to reasonably ascertain an individual's identity) that is collected, held, used or disclosed by Agilitus will be protected by the standards outlined in this Policy.

To comply with the current Australian laws and deliver on our commitment to privacy, Agilitus will:

- Abide by the APPs under the Act in relation to personal or sensitive information.
- Ensure that this Policy is freely and publicly available to all employees, stakeholders and any other interested parties to ensure that every person is aware of their requirements to comply with the Policy;
- Ensure lawful, non-discriminatory and unobtrusive methods are used to collect personal or sensitive information that is necessary for conducting business.
- Collect personal or sensitive information only with the individual's consent.
- Not disclose personal or sensitive information to an unrelated third party, except with the individual's consent or where Agilitus is required to do so by law;
- Destroy or de-identify personal or sensitive information in a secure manner when there is no further need for the information to be kept by Agilitus, or when required by law;
- Ensure only authorised employees who have agreed to maintain confidentiality have access to the information.
- Take reasonable measures to ensure that the personal or sensitive information stored by Agilitus is up to date, accurate and complete.
- Provide individuals with access to their personal or sensitive information on request and allow the individual to correct the information; and
- Periodically review and revise this Privacy Policy and related procedures to ensure it remains relevant and in compliance with the law.
- This Policy and related procedures ensure all personal or sensitive information stored by Agilitus is appropriately used and remains confidential.

1.1 What do we use personal or sensitive information for?

Personal or sensitive information is any information that can be used to identify an individual. Agilitus relies on personal or sensitive information for the effective management of our business, administrative, legal and corporate obligations.

Any personal or sensitive information provided to Agilitus will be used for the purpose of dealing with your request, enquiry or application for employment. This may involve disclosing your personal or sensitive information to any of the Agilitus offices internationally, the subsidiary

companies within Agilitus or to service providers who assist us in operating our business. These organisations are required to comply with the principles of this Policy.

By submitting your resume to Agilitus, you give us express consent to use, disclose and store your personal or sensitive information for the purposes of potential recruitment for a period of 12 months, at which point it will be destroyed. Any stored resumes will be secured from unauthorised access.

If your request is for Agilitus newsletters or other material, you can direct your e-mail to the relevant Agilitus office e-mail address (for example, info@agilitus.com). Your details and information about the newsletters, or the material you wish to receive will be held on our database and used for the purpose of administering your subscription or request. For all other enquiries, your details will only be available to and used by personnel dealing directly with your request. We do not use, or disclose, any personal or sensitive details you provide to us for direct marketing purposes.

1.2 What information do we collect?

Agilitus collects personal or sensitive information including but not limited to:

- Official and preferred names, titles, post-nominals, personal awards, address, telephone, e-mail and facsimile contact details (private and business), date of birth and next of kin;
- Qualifications, education and academic history, work experience and skills, previous occupations, previous employer information, areas of practice and areas of interest.
- Financial details including bank account information, superannuation details and tax file number;
- Contract of employment, resume and performance reviews; and
- Government-issued identifiers such as driver's license number.

Agilitus may also collect sensitive information, including:

- Membership information relating to professional groups and bodies; and
- Pertinent medical information such as known medical conditions and allergies.

Disclosure of medical information is completely voluntary (unless required by law) and is requested only to provide efficient care in the event of a medical emergency.

1.3 How personal or sensitive information is collected?

If reasonable and practicable to do so, personal, or sensitive information is collected directly from the individual. Agilitus aims to standardise the collection of personal or sensitive information through the use of forms however it is also often received through email, written notes, telephone conversations or face-to-face meetings.

Information that is obtained from an independent third party (such as a personal or work reference) is only collected in the event where the required information is not reasonable or practical to collect from the individual personally.

'Unsolicited information' refers to information that has been received without request by Agilitus. This information will only be held, used or released if it could have been collected through normal means. In the event that this is not the case, the information will be destroyed or de-identified as appropriate.

Agilitus also collects information through its website www.bge-resources.com. The site allows you to contact Agilitus through using the contact form for the purpose of requesting information about Agilitus or making other enquiries.

By submitting the contact form, you provide Agilitus with certain personal or sensitive information which may include your name, e-mail address and any other details you may choose to include. This information is collected by Agilitus for the purpose of dealing with your request. We may not be able to process your request without this information.

The Agilitus site uses "cookies" to gather and store your personal or sensitive information in accordance with the Australian Privacy Principles in the Privacy Act 1988.

1.4 How do we use personal or sensitive information?

Agilitus' primary use of personal or sensitive information is to ensure the efficient operation of the business. Personal or sensitive information is only used when reasonably necessary for a function or activity of the business, or when explicit consent of the individual has been sought and obtained. Potential uses of personal or sensitive information include but are not limited to:

- Assessing employment applications.
- Processing payments to employees and outside contractors;
- Communication with employees, previous employees, outside contractors, clients, stakeholders and people interested in communicating with Agilitus;
- Assisting in the day-to-day operations of the business including employee training, systems development, research and/or statistical analysis;
- Satisfying Agilitus' legal obligations including our duty of care; and
- Where necessary, marketing and promotional activities.

Personal or sensitive information is only collected when reasonably necessary for one or more of the above purposes and is only stored when the individual's consent is obtained.

1.5 Disclosure of personal or sensitive information

As noted above, we may share personal or sensitive information with related companies or with contractors carrying out services for Agilitus, who are required to comply with this Policy. Agilitus will only make such disclosures to accomplish the purpose for which the information was provided.

Otherwise, Agilitus' policy is not to disclose any personal or sensitive information to any unrelated third party except in the following circumstances:

- When your explicit consent has been obtained;
- To out related bodies corporate, and their respective directors, officers, agents and employees for the purposes of processing personal or sensitive information on our behalf (except in the case of sensitive information);

- To comply with any law enforcement agency, judicial proceeding, court order, or legal process in any jurisdiction that is investigating any breach or suspected breach of any law in any jurisdiction regarding your identity or other personal or sensitive information provided by you to us;
- Where we are permitted by law to disclose your personal or sensitive information;
- In the event of a medical situation or health emergency or;
- In the event of a serious non-medical emergency, such as a missing person situation

1.6 Storage and security of personal or sensitive information

Agilitus stores personal or sensitive information both electronically in various formats as well as in physical hard copies.

Electronic data is stored on a secure file server, on a secure network sitting behind a firewall with a hardened rule set. Backups of all digital information are taken on the hour, every hour and stored securely offsite within the Perth iX datacentre.

Agilitus employ various measures to ensure the protection of personal or sensitive information. These include, but are not limited to:

- Restricting access to personal or sensitive information to authorised employees based on their roles, responsibilities and hierarchy within the company;
- Educating all employees in the importance of maintaining the confidentiality of protected information, such as not revealing personal passwords or passcodes to anyone;
- Ensuring that all hard copy information is stored in locked cupboards and restricting access to only authorised employees;
- Utilising physical security measures such as the use of proximity cards logging access to and from all Agilitus offices and ensuring that the premises' are secured with monitored motion detecting alarm systems;
- Implementing policies and procedures in relation to protecting stored personal or sensitive information that is available for review by all employees.
- Ensuring that employees correctly follow protocols when handling personal or sensitive information by implementing human resources procedures such as confidentiality policies and email and internet usage guidelines; and
- Undertaking due diligence with respect to third parties who may have access to personal or sensitive information provided by Agilitus that they are compliant with the Act, the APPs and this policy.

When Agilitus no longer requires personal or sensitive information it is destroyed or de-identified as appropriate.

1.7 Accessing and updating personal or sensitive information

Upon request, Agilitus will provide you with access to your stored personal or sensitive information, unless there is an exception that applies under the APPs. This information will be provided as soon as is reasonably possible within 30 days from the date that the request is lodged. Depending on the nature of the request, providing the information may require longer than 30 days. If these circumstances arise, you will be notified in writing of the delay.

In certain circumstances, access to your personal or sensitive information may be refused. These circumstances could include, but are not limited to:

- Where the provision of the information may have an unreasonable impact on the privacy of other individuals;
- Access is denied by law;
- The request is regarded as frivolous or vexatious; or
- Any of the other seven provisions or circumstances as set out by the APPs.

In the event that Agilitus denies access to your personal or sensitive information, a detailed explanation will be provided.

Agilitus takes reasonable steps to ensure that the personal or sensitive information we have stored is accurate, complete and up to date. If personal or sensitive information we hold about you is inaccurate, incomplete or out of date, please let us know and we will make every effort to correct it. Employees can update their personal or sensitive information when any changes occur by logging into the secured Connx HRIS. Connx allows Agilitus employees direct access to their own human resources and payroll information. Each employee is supplied with their login details and password at the commencement of their employment. If you require help or more information, please contact Agilitus People and Culture team by e-mail hr@agilitus.com or phone +61 8 6375 9100.

1.8 Complaints and further information

If you have a complaint or require further information about how Agilitus handle personal or sensitive information or privacy issues please contact Agilitus Privacy Officer by e-mail privacy@agilitus.com or phone +61 8 6375 9100.

In the event of a complaint, the Privacy officer will confirm receipt of the complaint and will investigate the potential breach. Agilitus will endeavour to respond to any complaint within 30 days of original receipt. Further information may be sought from you in order to provide you with a comprehensive response. If you are not satisfied with the response that you have received from Agilitus, you are welcome to take your complaint to the Office of the Australian Information Commissioner. They may be contacted by email enquiries@oaic.gov.au or phone 1300 363 992.

1.9 Changes of this Privacy Policy

Agilitus may from time-to-time review and revise this Privacy Policy. We reserve the right to change this Policy at any time, whether in response to changes in Australian law or to shifts in company policy. We will notify you about any future changes by providing the up-to-date version on our website agilitus.com.



Craig Bloxham
Managing Director

