PRIVACY POLICY

1. We respect your privacy

1.1. Karen Barclay Virtual PA respects your right to privacy and is committed to protecting the privacy of our clients and website visitors. This policy sets out how we collect and treat your personal information.

1.2. We adhere to the Australian Privacy Principles contained in the *Privacy Act 1988* (Cth) and to the extent applicable, the EU General Data Protection Regulation (GDPR).

1.3. "Personal information" is information we hold which is identifiable as being about you. Personal information includes information such as your name, email address, identification number, or any other type of information that can reasonably identify an individual, either directly or indirectly.

1.4. You may contact us in writing at PO Box 2057, Essendon West, Vic. 3040 or by email kbarclay@karenbarclay-vpa.com for further information about this Privacy Policy.

2. Personal information collected

2.1. Karen Barclay Virtual PA will, from time to time, receive and store personal information you submit to our website, provided to us directly or given to us in other forms.

2.2. You may provide basic information such as your name, phone number, address, and email address to enable us to send you information, provide updates and process your service order. The information you provide will not be used for any purpose other than to respond to your enquiry or to provide you with our products or services.

2.3. We may collect additional information at other times, including but not limited to, when you provide feedback when you provide information about your personal or business affairs, change your content or email preference, respond to surveys and promotions, provide financial or credit card information, or communicate with our customer support.

2.4. Additionally, we may also collect any other information you provide while interacting with us.

3. How we collect your personal information

3.1. Karen Barclay Virtual PA collects personal information from you in a variety of ways, including when you interact with us electronically or in person, when you access our website and when we engage in business activities with you. We may receive personal information from third parties. If we do, we will protect it as set out in this Privacy Policy.

3.2. By providing us with personal information, you consent to the supply of that information subject to the terms of this Privacy Policy.

4. How we use your personal information

4.1. Karen Barclay Virtual PA may use personal information collected from you to provide you with information about our products or services. We may also make you aware of new and additional products, services, and opportunities available to you.

4.2. Karen Barclay Virtual PA will use personal information only for the purposes for which you consent. This may include to:

a) Provide you with products and services during the usual course of our business activities;

b) Administer our business activities;

c) Manage, research and develop our products and services;

d) Provide you with information about our products and services;

e) Communicate with you by a variety of measures including, but not limited to, by telephone, email, SMS or mail; and

f) Investigate any complaints.

4.3. We may disclose your personal information to comply with a legal requirement, such as a law, regulation, court order, subpoena, warrant, legal proceedings or in response to a law enforcement agency request.

4.4. If there is a change of control in our business or a sale or transfer of business assets, we reserve the right to transfer to the extent permissible at law our user databases, together with any personal information and non-personal information contained in those databases.

5. Disclosure of your personal information

5.1. Karen Barclay Virtual PA may disclose your personal information to any of our employees, officers, insurers, professional advisers, agents, suppliers, or subcontractors insofar as reasonably necessary for the purposes set out in this Privacy Policy.

5.2. If we do disclose your personal information to a third party, we will protect it in accordance with this Privacy Policy.

6. General Data Protection Regulation (GDPR) for the European Union (EU)

6.1. Where applicable, Karen Barclay Virtual PA will comply with the principles of data protection as set out in the GDPR for the purpose of fairness, transparency and lawful data collection and use.

6.2. We process your personal information as a Processor and to the extent that we are a Controller as defined in the GDPR.

6.3. We must establish a lawful basis for processing your personal information. The legal basis for which we collect your personal information depends on the data that we collect and how we use it.

6.4. We will only collect your personal information with your express consent for a specific purpose and any data collected will be to the extent necessary and not excessive for its purpose. We will keep your data safe and secure.

6.5. We will also process your personal information if it is necessary for our legitimate interests, or to fulfil a contractual or legal obligation.

6.6. You must not provide us with your personal information if you are under the age of 16 without the consent of your parent or someone who has parental authority for you. We do not knowingly collect or process the personal information of children.

7. Your rights under the GDPR

7.1. If you are an individual residing in the EU, you have certain rights as to how your personal information is obtained and used. Karen Barclay Virtual PA complies with your rights under the GDPR as to how your personal information is used and controlled if you are an individual residing in the EU.

7.2. Except as otherwise provided in the GDPR, you have the following rights:

a) To be informed how your personal information is being used;

b) Access your personal information (we will provide you with a free copy of it);

c) To correct your personal information if it is inaccurate or incomplete;

d) To delete your personal information (also known as "the right to be forgotten");

e) To restrict processing of your personal information;

f) To retain and reuse your personal information for your purposes;

g) To object to your personal information being used; and

h) To object against automated decision making and profiling.

7.3. Please contact us at any time to exercise your rights under the GDPR at the contact details in this Privacy Policy.

7.4. We may ask you to verify your identity before acting on any such request.

8. Hosting and International Data Transfers

8.1. Information that we collect may from time to time be stored, processed in or transferred between parties or sites located in countries outside of Australia. These may include, but not limited to the United States.

8.2. The hosting facilities for our website are situated in the United States. Transfers to each of these countries will be protected by appropriate safeguards including the use of standard data protection clauses adopted or approved by the European Commission which you can obtain from the European Commission Website.

8.3. Our Suppliers and Contractors are situated in the United States. Transfers to each of these countries will be protected by appropriate safeguards including the use of standard data protection clauses adopted or approved by the European Commission which you can obtain from the European Commission Website.

8.4. You acknowledge that the personal data you submit for publication through our website or services may be available, via the internet, around the world. We cannot prevent the use (or misuse) of such personal data by others.

9. Security of your personal information

9.1. Karen Barclay Virtual PA is committed to ensuring that the information you provide to us is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure information and protect it from misuse, interference, loss and unauthorised access, modification and disclosure.

9.2. Where we employ data processors to process personal information on our behalf, we only do so on the basis that such data processors comply with the requirements under the GDPR and that they have adequate technical measures in place to protect personal information against unauthorised use, loss and theft.

9.3. The transmission and exchange of information is carried out at your own risk. We cannot guarantee the security of any information that you transmit to us or receive from us. Although we take measures to safeguard against unauthorised disclosures of information, we cannot assure you that personal information that we collect will not be disclosed in a manner that is inconsistent with this Privacy Policy.

10. Access to your personal information

10.1. You may request details of personal information that we hold about you in accordance with the provisions of the *Privacy Act 1988* (Cth), and to the extent applicable the EU GDPR. If you would like a copy of the information which we hold about you or believe that any information we hold on you is inaccurate, out of date, incomplete, irrelevant or misleading, please email us at kbarclay@karenbarclay-vpa.com. We may ask you to verify your identity before acting on any such request.

11. Complaints about privacy

11.1. If you have any complaints about our privacy practices, please feel free to send in details of your complaints to kbarclay@karenbarclay-vpa.com. We take complaints very seriously and will respond shortly after receiving written notice of your complaint.

12. Changes to Privacy Policy

12.1. Please be aware that we may change this Privacy Policy in the future. We may modify this Policy at any time, in our sole discretion and all modifications will be effective immediately upon our posting of the modifications on our website or notice board. Please check back from time to time to review our Privacy Policy.

13. Website

13.1. When you visit our website

When you come to our website (https://www.karenbarclay-vpa.com/), we may collect certain information such as browser type, operating system, website visited immediately before coming to our site, etc. this information is used in an aggregated manner to analyse how people use our site, such that we can improve our service.

13.2. Cookies

We may from time to time use cookies on our website. Cookies are very small files which a website uses to identify you when you come back to the site and to store details about your use of the site. Cookies are not malicious programs that access or damage your computer. Most web browsers automatically accept cookies, but you can choose to reject cookies by changing your browser settings. However, this may prevent you from taking full advantage of our website.

13.3. Our website may from time to time use cookies to analyse website traffic and help us provide a better website visitor experience. In addition, cookies may be used to serve relevant ads to website visitors through third-party services such as

Google AdWords. These ads may appear on this website or other websites you visit.

13.4. *Third party sites*

Our site may from time to time have links to other websites not owned or controlled by us. These links are meant for your convenience only. Links to third party websites do not constitute sponsorship or endorsement or approval of these websites. Please be aware that Karen Barclay Virtual PA is not responsible for the privacy practices of other such websites. We encourage our users to be aware, when they leave our website, to read the privacy statements of each website that collects personal identifiable information.

26 March 2024

Cyber Security Policy

Karen Barclay Virtual PA is aware of the risk that cyber-attack poses to its business, and to the businesses of our clients. In particular, the risk of confidential or sensitive client information, both in hard copy and stored electronically. All team members, including employees and contractors, are required to adhere to this Cyber Security Policy.

Questions about the Policy should be directed to Karen Barclay, kbarclay@karenbarclay-vpa.com or 0432 015 716.

Your Responsibilities

Effective security is a team effort requiring the participation and support of every team member. It is your responsibility to know and follow these guidelines.

Anti-Virus Software

We use industry-standard anti-virus software to protect devices used to record and store confidential and private information.

Current protection is with BitDefender Zero Gravity Zone. Settings must be configured by our IT Contractor, TechSeek, to help prevent successful hacks and ransomware attacks.

All team members are to use only the IT equipment provided by Karen Barclay Virtual PA.

Password Policy

Strong passwords are key to ensuring security on devices, networks, and software. We enforce a strict Cryptographic password protocol with compulsory password manager use.

The current protocol is a minimum of eight (8) characters, including at least one upper case letter, lower case letter, number, and symbol. No use of dictionary words, including

compound words or combinations. No use of names, locations, or addresses. Avoid patterns, eg. sequential numbers or letters.

All team members need to be aware of their personal responsibilities for following the password policy.

Wherever possible, systems must be configured to enforce the password policy, eg. computer user accounts, Office 365, etc. and to enforce an account lockout policy, eg. three (3) failed attempts that will cause a user account to be locked.

Passwords must be changed immediately if a compromise is suspected.

Password sharing must be kept to an absolute minimum. Karen Barclay Virtual PA uses password management software, Bit Warden Password Manager, to share passwords, where required. All team members will have their own accounts. Passwords will only be shared using the authorised software, never by email or other insecure methods, such as via text message. Passwords must only be stored in the authorised management software and must never be written down or recorded elsewhere, such as in a hard copy document, such as a notebook, post-it-note, a Word document, or in an email.

Team members may choose to use a secure password generator within BitWarden Password Manager to generate passwords that meet the protocol.

Email Filtering

Karen Barclay Virtual PA uses Microsoft Office 365 email client, which incorporates multiple spam filters.

To maximise these protections, our IT Contractor, TechSeek will configure the protection settings to best meet the needs of Karen Barclay Virtual PA.

Web Traffic Filtering

Web traffic filtering is turned on for the office network.

Staff should ensure that web filtering is turned on if they are using a shared connection, such as a coworking space.

Bank Details

Where any bank details are provided by email in text format, ie. not PDF, such as an invoice or on a website, these are to be confirmed with the payee by phone before payments are made.

Two-Factor Authentication

Two-factor authentication, where available, is turned on for software programs used by Karen Barclay Virtual PA and its clients.

Users need an authentication app such as Google Authenticator or Microsoft Authenticator to sign in.

Software Updates

Karen Barclay Virtual PA use Windows 10 computers. It is essential that all software updates are performed in a timely manner, to minimise vulnerability to cyber-attack. All devices should be configured to automatically install updates, except over metered connections. If you are using a metered connection for an extended period, manually check and perform updates every week.

All staff must ensure that their devices and software are updated regularly to protect against the risk of cyber-attack.

Removeable Hardware

Karen Barclay Virtual PA does not use removable media to store or transfer information. We use OneDrive, Google Drive, or DropBox as file storage for the business. Files are stored on these cloud-based servers. Information is exchanged using protected mechanisms.

Use of removable hardware such as USB sticks is forbidden as they are vulnerable to being lost or stolen or introducing malware and viruses into the business.

Office Wireless Network

The office wireless network is a private internet connection. Accordingly, other members of the network cannot access your files.

It is preferable when working remotely that staff use a private internet connection.

Public Wi-Fi

A public Wi-Fi hotspot isn't required by law to be secure from potential online threats, so should be treated as unsecured, unless the operator of the hotspot states otherwise. Users can normally find this information in the security clause of the 'terms of use' that they typically must agree to before using a public Wi-Fi hotspot.

A public Wi-Fi hotspot that is password protected and uses Wi-Fi Protected Access 2 (WPA2) encryption and the 802.1x Standard for authentication, which is currently regarded as industry best practice, is considered secure.

Staff should avoid the use of public Wi-Fi hotspots. The office wireless network should be always used in the office, or if the network is unavailable, the staff member's personal hotspot may be used, and only if it is password protected. The next best alternative is to use a secured public hotspot.

Staff should avoid using an unsecured public Wi-Fi hotspot unless absolutely necessary and, in that case, any use should be limited to minimise the amount of confidential information exposed to the unsecured network, eg. turn off file sharing and location services.

Laptop Security

Work-related files should never be stored locally, except for syncing purposes. All work-related files are stored in the cloud-based storage provider, either the client's or Karen Barclay Virtual PA.

Back-Up

As all data is stored in the cloud-based storage provider of either the client or Karen Barclay Virtual PA, which has adequate protocols for data encryption in transit and at rest, it is not considered necessary at this point to add further back-up protocols. To do so may expose the business to additional data breach risk, eg. hacking of hard drive devices.

Karen Barclay Virtual PA has two SharePoint sites which are backed up to a Melbourne-based third-party data centre, AFI. Automated and fully encrypted backups are performed three times per day.

Training and Awareness

As part of the onboarding process, new staff are required to complete mandatory cyber security training.

Cyber Insurance

Karen Barclay Virtual PA has purchased a Cyber Risk Insurance Policy that provides us with cyber risk cover. This Cyber Risk Policy provides protection from losses to a limit of $250,000 for each claim. It provides cover for Network Security Liability, Privacy Liability, and Management Liability.

Cyber Risk Assessment

At the end of every financial year, Karen Barclay will review this policy, in collaboration with TechSeek, assess the business' exposure to cyber risk and update our policies and practices to address any change.

Changes to this Policy

Karen Barclay Virtual PA may update this policy from time to time to record our updated security procedures. This Cyber Security Policy was last updated in April 2024.