Connectivity I.T. Pty Ltd Privacy Policy

Last updated on 25/06/2018

About this Privacy Policy

This Privacy Policy describes how Connectivity I.T. Pty Ltd collects, holds, discloses and otherwise processes personal data and the steps that Connectivity I.T. Pty Ltd takes to secure the personal data that it holds. In this Privacy Policy, "***we***", "***our***" and "***us***" are all references to Connectivity I.T. Pty Ltd ABN 41128650635 of Level 1 5/15 Phoenix Street, Warragul VIC 3820.

We are committed to complying with our privacy obligations in accordance with all applicable data protection laws, including the Australian Privacy Principles contained in Schedule 1 to the *Privacy Act 1988* (Cth) (the "***Privacy Act***"). We comply with the EU General Data Protection Regulation ("***GDPR***") in relation to all personal data that we collect, hold, disclose and otherwise process, whether or not the personal data is within the scope of the GDPR ("***GDPR Data***").

If we decide to change this Privacy Policy, we will post the updated version on this webpage so that you will always know what personal data we gather, how we might use that information, and whether we will disclose it to anyone. If you are our client, we will notify you of any changes to our Privacy Policy by sending an email to you using the email address that we have for you on file.

What is personal data?

In this Privacy Policy, "personal data" has the meaning given to it in the GDPR.

Article 4(1) of the GDPR defines "personal data" as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The types of personal information we collect

Our policy is to minimise the amount of personal data we collect. Accordingly, we only collect personal data that is adequate, relevant and limited to what is necessary for the purpose for which it is to be processed and only where we are entitled by law to collect it. We may also use collected personal data for other related, directly related or compatible purposes (if and where permitted by applicable law).

We collect the following types of personal data:

- ***Contact details, transaction, employment and payment data***: We collect names, gender, job titles, telephone numbers, mobile phone numbers, email addresses, occupation, credit card details, tax file numbers, bank account details, records of products and services supplied to a person, postal addresses, residential addresses, business addresses, information contained in resumes and employment records such as employment history, education, qualifications, medical certificates, academic transcripts, salary details, superannuation account detail, and criminal record personal data contained in comments and feedback, personal preferences,. We will process this personal data in order to administer our client, employment and business relationships, to answer questions about and to provide and manage our services, and to otherwise enforce our rights and comply with our obligations.

- ***Client databases:*** In the course of providing our services we may host client databases or content specifically at the request of our clients, that our clients have provided to us. These databases and content may include any type of personal data.

- ***Managed services technical data:*** When providing our managed services, we may monitor or access our clients' computer, network and other equipment remotely or on site. In the course of doing so, we will collect and process information about that equipment and any software and data processed by that equipment. This information includes IP addresses, server names, database names, network names, serial numbers of equipment used, WiFi passwords, computer names, application names, browser history, user access logs, usernames, passwords, technical support log tickets, bandwidth used, error messages, social media handles, FTP server addresses, usernames and passwords, hostnames, subnet masks, router names, server addresses, hosting account usernames and passwords.

- ***Computer and network usage data:*** Subject to applicable laws, we may carry out electronic surveillance of our employees and contractors when they use our computer equipment, smartphone devices and networks to monitor compliance with company policies (including our Corporate IT Systems and Social Media Policy). This surveillance includes tracking and monitoring, reviewing and logging emails sent and received, websites visited, content viewed and files uploaded/downloaded. It also includes IP addresses, server names, database names, network names, serial numbers of equipment used, WiFi passwords, computer names, application names, browser history, user access logs, usernames, passwords, technical support log tickets, bandwidth used, error messages, social media handles, FTP server addresses, usernames and passwords, hostnames, subnet masks, router names, server addresses, hosting account usernames and passwords.

- ***Website analytics data:*** We collect and process personal data known as analytics data for analytical purposes, designed to measure and monitor how our websites are being used and to highlight any areas for improvement, optimisation and enhancement of our websites, including user location, IP addresses, cookie data, information about devices accessing our websites (IP address, the type of device used to access our websites and the operating system), the amount of time a user spent on our website and in which parts of it, and the path they navigated through it. We will process this personal data in order to monitor and detect unauthorised use of our websites, and to establish how our websites are used and to highlight areas for potential improvement of our websites. We often aggregate this data with other data. However, where the aggregated data is classified as personal information (or in the case of GDPR Data, personal data) we treat it in accordance with this Privacy Policy.

- **Cookies and other Tracking Technologies:** We use cookies and other tracking technologies (such as traffic analytics) on our websites for website functionality, performance and advertising purposes. We will not place such tracking technologies on your computer, smartphone or electronic device without your consent, unless they are required in order for us to provide the functionality supplied by our websites. If they are not installed, features of our websites may be unavailable and your experience may be impaired as a result. Cookies are pieces of information that a website transfers to a computer's hard disk for record-keeping purposes. We may use session cookies, which are only stored for a limited amount of time and persistent cookies that remain indefinitely until they are deleted. Such cookies may be installed by us or by our third contractors. Cookies enable us to remember and recognise you to better facilitate your user satisfaction when you visit our websites by helping us tailor and improve the information we present to you. The use of cookies is common in the Internet industry, and many major websites use them to understand your usage of websites, to customise websites for you, for statistical purposes and to provide useful relevant features, products, advertisements and services. A cookie may be used to tell when your computer or device has contacted our websites and extracts information such as your IP address, browsing pattern, content that you have viewed and browser type.

- ***Telecommunications Data:*** As an internet service provider, we are required to retain data about communications under Part 5-1A of the *Telecommunications (Interception and Access) Act* 1979 (**TIA Act**). This information is retained for 2 years from the date that we create it. We are also required under the TIA Act to retain subscriber information for 2 years from the date the relevant account is closed. The data that we retain in accordance with our obligations under the TIA Act may be disclosed to law enforcement agencies. The specific types of personal information that we may be required to collect and retain under the TIA Act are as follows:

Kinds of information to be kept		
Item	**Topic** **Column 1**	**Description of information** **Column 2**
1	The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	The following: (a) any information that is one or both of the following: (i) any name or address information; (ii) any other information for identification purposes; relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service; (b) any information relating to any contract, agreement or arrangement relating to the relevant service, or to any related account, service or device; (c) any information that is one or both of the following: (i) billing or payment information; (ii) contact information; relating to the relevant service, being information used by the service provider in relation to the relevant service; (d) any identifiers relating to the relevant service or any related account, service or device, being information used by the service provider in relation to the relevant service or any related account, service or device; (e) the status of the relevant service, or any related account, service or device.
2	The source of a communication	Identifiers of a related account, service or device from which the communication has been sent by means of the relevant service.
3	The destination of a communication	Identifiers of the account, telecommunications device or relevant service to which the communication: (a) has been sent; or (b) has been forwarded, routed or transferred, or attempted to be forwarded, routed or transferred.
4	The date, time and duration of a communication, or of its connection to a relevant service	The date and time (including the time zone) of the following relating to the communication (with sufficient accuracy to identify the communication): (a) the start of the communication; (b) the end of the communication; (c) the connection to the relevant service; (d) the disconnection from the relevant service.
5	The type of a communication or of	The following: (a) the type of communication;

Kinds of information to be kept		
Item	**Topic** **Column 1**	**Description of information** **Column 2**
	a relevant service used in connection with a communication	Examples: Voice, SMS, email, chat, forum, social media. (b) the type of the relevant service; Examples: ADSL, Wi-Fi, VoIP, cable, GPRS, VoLTE, LTE. (c) the features of the relevant service that were, or would have been, used by or enabled for the communication. Examples: Call waiting, call forwarding, data volume usage. Note: This item will only apply to the service provider operating the relevant service: see paragraph 187A(4)(c).
6	The location of equipment, or a line, used in connection with a communication	The following in relation to the equipment or line used to send or receive the communication: (a) the location of the equipment or line at the start of the communication; (b) the location of the equipment or line at the end of the communication. Examples: Cell towers, Wi-Fi hotspots.

We may also be required by law to intercept the content of communications made on our telecommunications networks and provide that content to law enforcement agencies. The types of data that may be intercepted may include websites visited, packets downloaded, connection duration, IP addresses, serial numbers of customer premises equipment used, and any other data transmitted via our networks and captured by our servers.

Who we collect personal data about

We collect personal data of:

- any person who contacts us with enquiries about our services, whether by email, through contact forms on our website, face to face or by telephone
- people who download whitepapers and other content from our website
- our officers, agents, employees and subcontractors
- our clients (and their officers, agents, employees and subcontractors)
- other parties to a transaction or dispute that we or our clients have entered into or are considering entering into or negotiating, and their representatives
- our suppliers (and their officers, agents, employees and subcontractors)
- individuals who participate in our surveys
- employees, potential employees, subcontractors, potential subcontractors and work experience applicants
- any person where it is necessary to do so in order to provide the services that we are engaged or instructed by our clients to perform

- the representatives of other service providers and other third parties who may contact us about our clients and who we deal with on behalf of our clients

How we collect personal information

We collect personal data in the following ways:

- when our clients and potential clients fill out forms with their personal data;
- when we take notes during meetings, interviews, telephone calls, conferences and events;
- through emails, letters and other correspondence and documents that we receive from clients, potential clients and others;
- when we are contacted by or communicate with any person online, through social media, email, communication tools such as Skype, online chat programs, blogs and the contact forms on our websites;
- when we are provided with completed surveys or questionnaires that we may distribute;
- when people apply for employment with us or offer to provide us with goods or services as suppliers and contractors (for example, potential employees will provide us with personal information that we will collect when they provide us with references, resumes and attend job interviews);
- when our employees, contractors and suppliers provide us with personal data;
- when our distributors, resellers and channel partners provide us with personal data that they collect about clients and potential clients;
- when we trade business cards with any person;
- when it is sent to us by our clients for the purpose of providing us with instructions or information necessary for us to process in order to provide services to our clients;
- when it is included in contracts that we enter into;
- through websites, public registers and directories such as telephone directories and business name and company searches;
- in the course of providing our services;
- when we obtain databases containing personal data that our clients provide us with so that we can provide services to them which rely on those databases;
- where any person voluntarily discloses it to us.

How we hold and use personal data

We hold personal data that we collect in our offices, computer systems, and third party owned and operated hosting facilities. We use personal data for the following purposes:

- in order to verify a person's identity when we are contacted to ensure that we know who we are communicating with;

- to communicate with our and our potential clients, employees, subcontractors, suppliers and colleagues, whether by telephone, email, post or otherwise;

- to provide clients with our services and to administer, maintain and answer questions about our services;

- in order to send newsletters and other communications to our clients concerning our services, events and business opportunities;

- to send marketing material to clients and other individuals in our newsletter database who we believe may be interested in the content of our marketing material;

- to enforce our rights and comply with our contractual and other legal obligations;

- to issue bills and invoices to our clients and others, and to enforce the payment obligations of our clients to pay our fees;

- in order to consider a person as a potential employee or contractor (for example, by checking a person's references or considering the persons' resume and arranging interviews) and to pay our employees and contractors their wages, salaries, service fees and other entitlements;

- when conducting publicity campaigns;

- to handle complaints;

- to manage employee records;

- in order to process an application for our services;

- to identify customers and other individuals when we are contacted with questions or concerns regarding the products and services we provide;

- in order to configure a new service for our customers;

- when conducting research and development of our products and services;

- in order to conduct checks for credit worthiness;

- for direct marketing purposes.

Who we disclose personal data to

We will only disclose personal data that we collect to third parties as follows:

- ***To our suppliers who host our files and databases in the cloud*** – we store backup copies of our computer files, software and databases in the cloud with our hosting providers who host those files, and that software and databases (including any personal data contained in them) on our third party hosting providers' computer servers located in their data centres;

- ***To hosting providers who host our clients' databases and content*** – where necessary or practical to do so for the purposes of providing services to our clients or for the purposes of operating our business, we hold our clients' databases and content (including any personal data contained in them) on third party computer servers in the data centres of our hosting providers;

- ***To other parties to a commercial arrangement where necessary in order to provide our services*** – for example we may need to supply your name to the professional advisors of other parties who you are dealing with (or any regulator) where we agree to represent you or provide you with services with regards to any matter, including but not limited to, where a client authorises us to do so we may need to provide the client's personal data to its agents or other professional advisors;

- ***To our resellers, distributors, agents and channel partners –*** we may appoint resellers, distributors, agents and channel partners to sell our products and services, or to manage parts of our business for us. In the course of those relationships, we may provide client or potential client personal data to them, or they may provide client or potential client personal data to us that they have collected for us;

- ***So that we can obtain assistance from our suppliers and corporate group*** with the provision of our services – in which case we may disclose your personal data to our suppliers and subcontractors as well as to members of our corporate group who we may subcontract the provision of all or part of our services to. For example, we may use printing providers who print documents on our behalf, couriers who deliver documents on our behalf which contain personal data, and share computers which contain personal data with our related bodies corporate;

- ***Conducting publicity campaigns*** – in which case we may disclose your personal data to our marketing suppliers;

- ***Handling claims, legal disputes and complaints*** – in which case we may disclose your personal data to our insurers, lawyers, accountants and other professional advisors;

- ***Sending out a newsletter*** – in which case we may disclose your personal data to our email and newsletter service providers;

- ***In order to identify our Customers and end users*** - when we are contacted with questions or concerns regarding the products and services that we provide;

- ***In order to record billing details and process payments from our clients*** – in which case we will provide client bank account, cheques and credit card details to our bank and merchant facility providers;

- ***For professional advice*** - when providing information to our legal, accounting or financial advisors/representatives or debt collectors for debt collection purposes or when we need to obtain their advice, or where we require their representation in relation to a legal dispute;

- ***If we sell the whole or part of our business or merge*** with another entity – in which case we will provide to the purchaser or other entity the personal data that is the subject of the sale or merger;

- ***Where a person provides written consent to the disclosure*** of his or her personal data***;***

- ***Where required by law.***

We may also provide your personal data to our lawyers, insurers and professional advisors and any court or administrative body, for one or more of the following purposes:

- To obtain or maintain insurance;

- The prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

- To protect or enforce our rights or defend claims;

- Enforcement of our claims against you or third parties;
- The enforcement of laws relating to the confiscation of the proceeds of crime;
- The protection of the public revenue;
- The prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
- The preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of the court or tribunal.
- Where disclosure is required to protect the safety or vital interests of employees, end users or property.

Notifiable data breaches

Since 22 February 2018, data breaches that are likely to result in serious harm must be reported to affected individuals and the Office of the Australian Information Commissioner (**OAIC**), except where limited exceptions apply. For the purposes of the GDPR, certain types of data breaches must also be reported to affected individuals if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms. In addition, the GDPR requires organisations to report certain types of data breaches to the relevant supervisory authority. We will notify affected individuals, the OAIC and relevant supervisory authorities of any data breach where we are required to do so in accordance with our legal obligations.

Automated decision making

We do not use automated-decision making in our business.

Lawful basis of processing

Under the GDPR, GDPR Data can only be processed where there is a lawful basis to do so. We will only process GDPR Data where we have a lawful basis to do so. Except where specified otherwise in this Privacy Policy to the contrary or implied in this Privacy Policy to the contrary, we will only process personal data where necessary for our legitimate interests or the legitimate interests of a third party, or where we are required to do so pursuant to a contract or other legal obligation.

Third party websites and platforms

Our websites may include links to third party websites and platforms. Our linking to those websites and platforms does not mean that we endorse or recommend them. We do not warrant or represent that any third party website or platform operators comply with applicable data protection laws. You should consider the privacy policies of any relevant third party websites and platforms prior to sending your personal data to them.

You may interact with social media platforms via social media widgets and tools such as the Facebook Like button and the Facebook pixel that may be installed on our websites. These widgets and tools may collect your IP address and other personal data. Your interaction with such widgets and tools, and any single sign-on services such as Open ID is governed by the privacy policies of the relevant social media operators and single sign-on service providers – please read them so that you are aware of how they process your personal data.

Security

We take reasonable steps to protect personal data that we hold from unauthorised access, modification and disclosure and implement technical and organisational measures to ensure a level of protection

appropriate to the risk of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, as follows:

- We perform security testing (including penetration testing of our websites), and maintain other electronic (e-security) measures for the purposes of securing personal information, such as passwords, anti-virus management, multi-factor authentication, firewalls and antivirus software

- We maintain physical security measures in our buildings and offices such as door and window locks and visitor access management, cabinet locks, surveillance systems and alarms.

- We require all of our employees and contractors to comply with privacy and confidentiality terms and conditions in their employment contracts and subcontractor agreements that we enter into with them.

- We carry out security audits of our systems which seek to find and eliminate any potential security risks in our electronic and physical infrastructure as soon as possible

- If appropriate in the circumstances, taking into account the state of the art, the costs of implementation and the nature, scope, content and purpose of the processing, we pseudonymize and/or encrypt personal data

- We implement passwords and access control procedures into our computer systems

- We have a Data Breach Response Plan in place

- We have data backup, archiving and disaster recovery processes in place

- We have anti-virus and security controls for email and other applicable computer software and systems in place

- We have processes in place to ensure integrity and resilience of systems, servers and personal data

- We have processes for regular testing, accessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

Privacy Tools

Our websites include privacy tools that you can use to control how we process personal data that we hold on our customers' behalf. Customrs can access these privacy tools at the following URL: https://my.dcsi.net.au/

If you refuse to provide us with personal data

If you do not provide us with your personal data, you can only have limited interaction with us. For example, you can browse our website without providing us with personal information, such as the pages that generally describe the services that we make available, and our Contact Us page. However, when you submit a form on our website, or become a client or otherwise enter into a business relationship with us, we need to collect personal data from you in order to identify who you are, so that we can provide you with services, and for the other purposes described in this Privacy Policy. You have the option of not identifying yourself or using a pseudonym when contacting us to enquire about our services, but not if you wish to actually obtain our services. It is not practical for us to provide you with our services if you refuse to provide us with personal data.

Spam email

We do not send "junk" or unsolicited e-mail in contravention of the *Spam Act 2003* (Cth). We will, however, use e-mail in some cases to respond to inquiries, confirm purchases, or contact clients. These transaction-based e-mails are automatically generated. Anytime a client or visitor receives e-mail it does not want from us they can request that we not send further e-mail by contacting us via email at: support@dcsi.net.au or using any 'unsubscribe' tool contained in any communication we send. Upon receipt of any such request, we will ensure that they cease to receive automated emails from us.

Offshore data transfers

We may transfer your personal data to our contractors and service providers who assist us with providing our products and services to you, and to assist us with the operation of our business generally, where we consider it necessary for them to provide that assistance.

Provided that we comply with applicable law, including the provisions of Australian Privacy Principle 8 (Cross-border disclosure of personal information), and the GDPR – in relation to GDPR Data, we may transfer your personal data to our offshore contractors and service providers as well, who may be located outside the European Union (EU) or the European Economic Area (EEA). At present, we do not transfer personal data out of Australia.

We will only engage new third parties to process GDPR Data that you instruct us to process as a processor on your behalf if you have authorised us to do so pursuant to a specific or general written authorisation and otherwise in compliance with the requirements of the GDPR.

Retention and de-identification of personal data

It is our policy to retain personal data in a form which permits identification of any person only as long as is necessary for the purposes for which the personal data was collected; and for any other related, directly related or compatible purposes if and where permitted by applicable law. We will only process personal data that you provide to us for the minimum length of time permitted by applicable law and only thereafter for the purposes of deleting or returning that personal data to you (except where we also need to retain the data in order to comply with our legal obligations, or to retain the data to protect your or any other person's vital interests). Where you require personal data to be returned, it will be returned to you at that time, and we will thereafter delete all then remaining existing copies of that personal data in our possession or control as soon as reasonably practicable thereafter, unless applicable law requires us to retain the personal data in which case we will notify you of that requirement and only use such retained data for the purposes of complying with those applicable laws.

Where the personal data is not GDPR Data and is personal information for the purposes of the *Privacy Act 1988* (Cth), instead of destroying the personal information we may take such steps as are reasonable in the circumstances to de-identify the personal information that we hold about an individual where we no longer need it for any purpose for which it may be used in accordance with this Privacy Policy if the information is not contained in a Commonwealth record and we are not required by Australian law (or a court or tribunal order) to retain it.

Your rights under the GDPR

Under the GDPR, you have a number of rights, including:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Please contact us if you wish to exercise any of your rights under the GDPR. We will handle all such requests in accordance with our legal obligations. If you withdraw your consent for processing, object to the processing of your personal data or request us to erase your personal data and as a result, it is not possible or practical for us to continue providing you with our services, we may elect to terminate our business relationship with you.

How to access and correct personal data held by us

Please contact us if you wish to access the personal data that we hold about you, using the details set out at the end of this Privacy Policy. We will handle your request for access to your personal data in accordance with our statutory obligations. To ensure that we only obtain, collect, use and disclose accurate, complete and up to date personal data, we invite you to contact us and inform us if any of your personal details we hold change or if any of the personal data held by us is otherwise incorrect or erroneous. In exchange for your payment to us of a reasonable fee, we will provide you (or if you wish, another controller) with a copy of the personal data they we hold about you in a structured, commonly used and machine readable format. However, we will not charge any fee to access your GDPR Data where the GDPR prohibits us from doing so.

Our contact details

We are Connectivity I.T. Pty Ltd ABN 41128650635 of Level 1 5/15 Phoenix Street, Warragul VIC 3820. If you wish to contact us for any reason regarding our privacy practices or the personal data that we hold about you, please contact us at the following address:

Privacy Representative
$100
Managing Director
PO Box 801, Warragul VIC 3820
privacy@connectivityit.com.au

Data Protection Officer
Jacob Carr
Data Protection Officer
Connectivity I.T. Pty Ltd
PO Box 801, Warragul VIC 3820
privacy@connectivityit.com.au

We will use our best endeavours to resolve any privacy complaint within ten (10) business days following receipt of your complaint. This may include working with you on a collaborative basis to resolve the complaint or us proposing options for resolution.

If you are not satisfied with the outcome of a complaint or you with to make a complaint about a breach of the Australian Privacy Principles you make refer the complaint to the Office of the Australian Information Commissioner (OAIC) who can be contacted using the following details:

Call: 1300 363 992
Email: enquiries@oaic.gov.au
Address: GPO Box 5218, Sydney NSW 2001

In relation to GDPR Data, you may lodge a complaint with any relevant supervisory authority.