

Privacy Policy and Site Terms and Conditions



About this policy

Version as at July, 2020

The Privacy Act 1988 requires entities such as Barefoot Media Solutions (BMS) to have a privacy policy. This Privacy Policy outlines the personal information handling practices of BMS. This Policy is written in simple language. The specific legal obligations of BMS when collecting and handling your personal information are outlined in the Privacy Act 1988 and in particular in the Australian Privacy Principles in that Act. We will update this Privacy Policy when our information handling practices change. Updates will be published on our website.

Overview

WebTragics Pty Ltd is the parent company that trades as Barefoot Media Solutions (BMS). It operates for profit, privately held and located in Hobart Tasmania. BMS provides digital strategy services, social media consulting to businesses, photography, video and other digital services as depicted on this website.

We recognise that the scope and scale of our company means that we touch many lives. As a business, this is not something that we ever take lightly.

Protecting your privacy and the confidentiality of your personal information is fundamental to the way BMS does business.

This Privacy Policy explains how BMS will manage and protect your personal information, including information that BMS collects during the course of providing a product or service to you and the information BMS holds after your product or service is terminated (where we are required to hold this information or it is necessary for our functions).

This Privacy Policy contains information about how you can access the information BMS holds about you, how you can ask BMS to correct your information, and how you can make a complaint if you have concerns about how BMS has managed your information.

At the time of publication the BMS consists of the following businesses each of which are bound by this Policy:

Barefoot Media Solutions(BMS)

- Head Office: Level 2 #162 Macquarie Street Hobart, TAS, 7000

ABN: 45 062384105

ACN: 062384105

Collection of your personal information

At all times we try to only collect the information we need for the particular function or activity we are carrying out.

The main way we collect personal information about you is when you give it to us. For example, we collect personal information where required to provide surveys, questionnaires, digital strategy fact finding services and email contact forms.

Such personal information may comprise of one or more of the following:

- Your name, address, date of birth contact details;
- Business name;
- Video footage;
- Your stated or likely preferences, for example whether you may be interested in particular products, services, or promotions; or
- Information about your opinions and what you like.

We will also collect information that you provide us when signing up to mailing lists and registering for our events, or when submitting feedback on your experience with our websites.

Further, BMS may collect information from you because we are required or authorised by an Australian law, or court or tribunal to collect that information.

Collecting sensitive information

Sensitive information is personal information about a person's racial or ethnic origin, political opinion, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, criminal record, genetic information or health information.

BMS will not collect, use or disclose sensitive information about you unless we need the information for one of our functions or activities and we have your consent (or we are legally required to do so).

For example, we may collect personal information to aid in the application process for a third party payment gateway that requires integration with a website we have built on your behalf.

Indirect collection

There may be occasions when we collect personal information about you from a third party. For example, we may collect personal information from:

- Credit reporting bodies if we request a report about your credit history;
- Other credit providers if we request information from them about the products they provide you;

- Organisations that we have an arrangement with to jointly offer products and/or has an alliance with to share information for marketing purposes to provide you with products or services and/or to promote a product or service;
- Marketing companies if we acquire contact information to tell people about our products and services that may interest them; or
- Other parties who may have introduced you to one or more of our businesses.

Further, in the course of handling and resolving a complaint, data breach, review or an investigation we may collect personal information (including sensitive information) about you indirectly from publicly available sources or from third parties such as:

- Your authorised representative, if you have one; or
- Applicants, complainants, respondents to a complaint, investigation, application or data breach notification or the third parties' employees and witnesses.

Third party sites and services

Our websites, products, applications, and services may contain links to third-party websites, products, and services. Our products and services may also use or offer products or services from third parties. These websites may store information across multiple countries.

Information collected by third parties, that may include such things as location data or contact details, is governed by their privacy practices. We encourage you to learn about the privacy practices of those third parties.

At the time of publication our Service Providers and Partners include:

Analytics:

- Google Analytics

Hosting Services:

- Webtragics
- Site5
- Drop-box
- OneDrive

Human Resources:

- Employsure

Online Bookings:

- Eventbrite

Survey / Campaign Management:

- Survey Monkey
- Mailchimp

- InVision

Social Media:

- Facebook
- Instagram
- YouTube
- Twitter
- Google Business

Information we collect automatically

Whenever you visit or interact with any of our websites, we as well as any third party service providers may use a variety of technologies that automatically or passively collect information about how our websites are accessed and used [‘Usage Information’].

Usage Information may include, in part, browser type, operating system, the page served, the time and the preceding page views. This statistical data provides us with information about the use of our websites, such as how many visitors visit a specific page, how long they stay on that page, and which hyperlinks, if any, they ‘click’ on. Usage Information is non-identifying, but if we are to associate it with you as a specific and identifiable person, we then treat it as Personal Information.

We may also automatically collect your IP address or other unique identifier [‘Device Identifier’] for the computer, mobile device, technology or other device [collectively, ‘Device’] you use to access our websites.

A Device Identifier is a number that is automatically assigned to your Device when you access a website or its servers, and our computers identify your Device by its Device Identifier.

The technologies used on our websites to collect Usage Information, including Device Identifiers, may include:

Cookies

Cookies are data files placed on a Device when it is used to visit our websites. We may place cookies or similar files on your Device for security purposes, to facilitate site navigation and to personalise your experience while visiting our websites. Cookies allow us to collect technical and navigational information, such as browser preferences. However, please be aware that some features of our websites may not function properly or may be slower if you refuse cookies.

Pixels

Small graphic images or other web programming code called pixels, may be included in our websites and email messages. Pixels or similar technologies may be used for a number of purposes, including, without limitation, to count visitors to the websites, to monitor how users navigate the websites, to count how many emails that were sent were actually opened or to determine whether content sent was actually viewed.

Social networking services

We use social networking services such as Facebook, Instagram, Twitter, YouTube, and Google Business to communicate with the public about our work. When you communicate with us using these services we may collect your personal information, but we only use it to help us to communicate with you and the public. The social networking service will also handle your personal information for its own purposes. These services have their own privacy policies. You can access the privacy policies for [Facebook](#), [Instagram](#), [Twitter](#), and [YouTube](#) (a Google company) on their websites.

Your consent is important.

BMS may require your consent to use and/or disclose your information in particular ways. Your consent may either be inferred or expressed.

Inferred Consent is

- By an existing relationship you have with our properties or businesses, or
- Where there is a reasonable expectation of you receiving commercial electronic messages from us, or
- Where you have published a work related email that is accessible to the public or a section of the public.

Expressed consent is for example:

- By filing out a form, ticking a box on a web site, over the phone, face-to-face, swapping business cards, or
- As long you are aware that you may receive a commercial electronic message from us.

If you no longer want to receive our offers, information on our services and other promotional activities you can 'opt-out', or 'unsubscribe' from any of our commercial electronic messaging such email, SMS, MMS or IM, or contact us directly.

Collection of images

From time to time BMS will hold events where images are likely to be taken for various promotion, electronic publications, and surveillance purposes.

We will at all times ensure to provide as much detail as possible about what the image will be used for and who will be able to see it. By entering a BMS event, customers:

- Consent to the recording of their image, likeness or voice by any means (including such things as video, audio and visual recordings by television cameras and photographers, [together 'Images']); and
- Consent to the use of the Images at the event, including display on vision screens throughout the event.

The use of cameras including mobile phones with camera interfacing is not permitted in the specified public areas of the event such as change rooms and toilets.

Video surveillance

We are committed to providing a secure environment for all visitors to our properties. Our premises and their surroundings are under constant surveillance. Surveillance video is only retained for a specified period of time except where its retention for a longer period is required to assist the investigation of unlawful, suspicious activities or defence of claims against BMS. Details of suspected illegal and undesirable activities are shared with law enforcement bodies and regulatory bodies.

Children's privacy

BMS will use particular care in the handling the images and other personal information of children. Depending on the age and ability of the child to understand our explanation about what is going to happen with their image and to make a truly informed choice, BMS will discuss these things with their parent or guardian first.

If BMS becomes aware that personal information that has been collected relates to a child without the consent of a parent or guardian, we will use reasonable efforts to:

- Delete that personal information from its files as soon as possible; and
- Ensure where deletion is not possible, that this personal information is not used further for any purpose, nor disclosed further to any third party.

BMS will also meet the requirements of any other legislation that protects children.

All members of the BMs team will carry and ensure valid WWVP licensing is in place at all times.

Disclosure

Personal information is only used within BMS in the provision of services for which it was obtained and may be used to provide customers, through direct marketing, with knowledge of other services and promotions conducted by BMS. Your personal information is not sold or passed on to third parties for their marketing purposes.

Disclosure to service providers

BMS uses a number of service providers to whom we disclose personal information. These include providers that we have partnered with to provide health services, or other providers who host our website servers, manage our accounting, manage our IT, undergo research, and manage our human resources information.

To protect the personal information we disclose we:

- Enter into a contract or MOU which requires the service provider to only use or disclose the information for the purposes of the contract or MOU; and
- Include special privacy requirements in the contract or MOU, where necessary.

Disclosure of sensitive information

We only disclose your sensitive information for the purposes for which you gave it to us or for directly related purposes you would reasonably expect or if you agree, for example, to handle a complaint, or where we respond to a distress call or you request participation in certain tour activities.

Disclosure of personal information overseas

BMS may need to disclose your information to organisations located overseas. From time to time we may choose to use online solutions located overseas to perform direct marketing, undertake surveys, and store data. Also, we only disclose your information to these overseas organisations when it is necessary for the services they provide to BMS.

When we disclose your information overseas, we are required to take measures to ensure your information is treated in accordance with the standards that apply in Australia.

Quality of personal information

To ensure that the personal information we collect is accurate, up-to-date and complete we:

- Record information in a consistent format;
- Where necessary, confirm the accuracy of information we collect from a third party or a public source;
- Promptly add updated or new personal information to existing records; and
- Regularly audit our contact lists to check their accuracy.

We also review the quality of personal information before we use or disclose it.

Storage and security of personal information

BMS protects your personal information from misuse and loss. We also protect it from unauthorised access, modification and disclosure by ensuring that your personal information can only be accessed by people properly authorised to have access.

We will retain your personal information for the period necessary to fulfil the purposes outlined in this Privacy Policy unless a longer retention period is required or permitted by law.

Accessing and correcting your personal information

Under the Privacy Act (Australian Privacy Principles 12 and 13) you have the right to ask for access to personal information that we hold about you, and ask that we correct that personal information. You can ask for access or correction by contacting us and we must respond within 30 days. If you ask, we must give you access to your personal information, and take reasonable steps to correct it if we consider it is incorrect, unless there is a law that allows or requires us not to.

We will ask you to verify your identity before we give you access to your information or correct it, and we will try to make the process as simple as possible. If we refuse to give you access to, or correct, your personal information, we must notify you in writing setting out the reasons.

If we make a correction and we have disclosed the incorrect information to others, you can ask us to tell them about the correction. We must do so unless there is a valid reason not to.

If we refuse to correct your personal information, you can ask us to associate with it (for example, attach or link) a statement that you believe the information is incorrect and why.

Notifiable data breaches

From 20 July 2020, if we become aware of a suspected personal information data breach we will conduct an appropriate assessment to determine if there is a likely risk of serious harm to any individual associated with the data breach. Where we believe there is a likely risk of serious harm, we will notify the Office of the Australian Information Commissioner and any affected individuals in accordance with our obligations under the law.

How to make a complaint

If you wish to complain to us about how we have handled your personal information you should do so in writing. If you need help lodging a complaint, you can contact us.

If we receive a complaint from you about how we have handled your personal information we will determine what (if any) action we should take to resolve the complaint.

We will tell you promptly that we have received your complaint and then respond to the complaint within 30 days.

If you are not satisfied with our response you may ask for a review by a more senior Management Official (if that has not already happened), or you can access an external dispute resolution service, or apply to the Office of the Australian Information Commissioner (OAIC) to have your complaint heard and determined. The Privacy Commissioner may be contacted at: www.oaic.gov.au, or email: enquiries@oaic.gov.au

We may give a copy of the complaint or application to the Office of the Australian Information Commissioner, or other regulatory body or law enforcement agency as required by law.

How to contact us

If you have any questions or would like more information about this Privacy Policy you may contact the Programs & Operations Manager by email or post:

Email:

hello@barefootmedia.solutions

Post:

Barefoot Media Solutions

162 Macquarie Street HOBART TAS 7052

Changes in the future

We reserve the right to change our Privacy Policy at any time. All changes will be notified by posting an updated version of the Privacy Policy on our websites. Any changes to our Privacy Policy shall be deemed to take place on the date the changes are posted on our websites.