Internal FCTG Privacy Notice

1. Background and scope

Flight Centre Travel Group and its related subsidiaries and affiliates ("FCTG") collects and stores your personal information. This is an obligation we take very seriously, and we are firmly committed to protecting the privacy and confidentiality of your personal information.

This document, known as the Internal Privacy Notice, sets out how FCTG processes (i.e., collects, stores, and uses) your personal information. It applies to everyone employed by FCTG regardless of the business or brand you work for within the wider group.

When it comes to processing your personal data, FCTG is what is known as a "data controller". This term (or similar alternatives) is defined in the privacy legislation of many of the countries we operate in, and in practice means that FCTG determines what personal data is collected, and how it is used.

However, this does not mean that FCTG can simply do whatever it wants when it comes to the collecting and processing of your personal data. FCTG must abide by the data protection principles and requirements set out in the national privacy laws of the country you are a resident in. These often include:

- Only collecting personal data for legitimate purposes, and even then only collecting such data that is needed to achieve these purposes.
- Deleting or anonymising your personal data once these purposes have been met and it is no longer necessary to keep processing your personal data in a way that can identify you.
- Making sure any personal data we collect is accurate, stored in a secure manner, and that we are clear and transparent with you about what personal data we are collecting and why we are collecting it. This Notice is one of our key ways of providing you this transparency.

Please know that if ever your local data protection laws impose more restrictive obligations on FCTG than the practices set out in this Notice, we will adjust our practices in your state or country to make sure we continue to comply with your local data protection laws.

2. What personal information do we collect?

The exact meaning of personal information may vary slightly under your local data protection laws, but in general terms it means information which relates to a living person who can be identified from that information. So for example, your name, email address and your image all become personal information about you as they help identify who you are, especially when these three elements are combined together. This also extends to other types of information when linked to you, such as your salary, performance data, even your opinions.

In this section we set out the different categories of personal information FCTG can possibly collect on its employees. But to be very clear here, there *will be* variations as to the exact data we collect on each employee. This is influenced by things like an individual's role, the systems they access, the devices they use, the country they are employed in and any applicable laws in those countries which may prohibit the collection of such data.

If the country or state you are employed in prohibits FCTG from collecting and using either a data category and/or specific types of data within that category in relation to its employees, that data will not be collected or used. Please speak to your Privacy team (section 14 below) or Peopleworks if you have specific questions on this point.

FCTG will update this Internal Privacy Notice when we change the types of personal information elements we collect on you or make changes to how we use this data.

Data category	Examples of the types of data within the category
Identifiers (offline)	Name, date of birth, nationality, sex, gender, pronoun, place of birth.
Identifiers (online)	Such as IP address, device data, system specific user identifiers, and network information.
Work identifiers	Such as employee number, job title.
Family information	Marital status, information on employee's children (i.e., name, date of birth).
Contact information (home)	Such as residential/mailing address, personal/home telephone number, personal email address.
Contact information (work)	Such as work mailing address, work telephone number, work email address.

Government issued forms of identification	Such as passport details, national identity card details, driver's license details, tax file numbers, national insurance numbers, social security numbers, visa information, work permits and sponsorship details.
Banking, payment card and tax information	Such as bank account details, tax codes, student loan or higher education contribution details, credit/debit card details (including card type, card number, security number and expiry date and other financial details necessary to process various transactions), etc.
Pre-employment checks	Information requested during the employment process such as references, education transcripts, employment checks, background checks, credit checks, and the outcomes of assessments undertaken by our third party vendors who conduct checks on behalf of FCTG.
Emergency contact information	Such as name, email, telephone numbers, of designated emergency contacts.
Medical and health & safety information (physical and mental)	Such as health conditions and medical information disclosed by the employee either prior to or throughout the course of their employment, information on accidents at work, special working requirements, etc.
Financial information	Such as wages, pensions, superannuation, share schemes, benefit schemes, etc.
Human resource files (containing professional and employment-related information)	Such as contracts, work eligibility, agreed working arrangements, work history, performance reviews, dispute information and recorded outcomes.
Data identifying an individual's location	Such as residential and work addresses, IP addresses, device location information, travel itineraries, building and door access information, information recorded in system logs, etc.
Biometric data	Such as call recordings, images and photographs, fingerprint data, and CCTV recordings*. **Please note that many countries and states either prohibit or put additional restrictions around, the collection and use of certain types of biometric data that may include some of the examples listed here. As stated at the start of this section, FCTG will comply with all such legal restrictions that apply.*
Performance data	Such as sales data, completion of activities data, satisfaction data recorded from customer feedback (whether internal or external), achievement of any set targets or KPI's, local/regional/global dashboards showing performance data, output of data models (including those generated using machine learning and AI technologies), etc.
Work history	Such as human resources files, contracts, agreed working arrangements, investigations and dispute information and recorded outcomes, employment history within FCTG (roles, employment start and finish dates).
Travel information	Passenger name record (PNR) data, flight dates and routings, flight numbers, hotel reservations, car rental bookings, rail bookings, ticketing information, authorisation solutions and travel risk management
Communication data	Such as call recordings, emails, transcripts, Teams messages, phone use records, etc.
System and network generated data	Every interaction you have with systems, networks, and devices may be captured and recorded. This includes data points like recordings of actions undertaken by the user when using systems or applications, web browsing activities, logon activities (location, date/time), etc.
Diversity information	Ethnicity, sexual orientation, religious or philosophical beliefs, mental or physical health conditions or impairments
Training information	Records of training activities, records of acknowledgements by individuals of having completed and/or understood training materials, records of acknowledgements by individuals committing to complying with mandated work requirements.
Customer/client interaction information	Such as customer reviews of the service provided by a consultant, customer satisfaction surveys/reviews/responses, Voice of Customer surveys, and feedback by clients/customers that identifies the FCTG consultant, etc.

Employee survey responses	Responses by employees to non-anonymous work surveys and questionnaires.

3. How do we collect personal information, and what legal mechanisms do we rely upon when doing so?

FCTG will not collect personal information on you if doing so would be in breach of your local laws. And when we do collect, retain, and use your personal information we make sure this is done in compliance with your local data protection laws and other applicable local laws. The personal information that we do collect is generated from a number of different sources:

- Predominantly it is generated from your own actions, whether directly (e.g., when you provide us your personal information, either voluntarily or as a requirement of your employment) or indirectly (i.e., via your interactions with FCTG's customers, other employees, systems, and operational processes).
- It can be generated directly by other FCTG employees, our clients, or customers.
- It can be generated by the systems, websites and applications you use. It can also be generated by physical systems/devices, like laptops, phones, CCTV cameras, and security doors.
- Your personal data may also be provided to us via third parties, such as information collected on you, or verified about you. Primarily this will occur during your recruitment process, but it may also occur periodically and/or on an as-needs basis during the course of your employment within FCTG.

Depending on the privacy laws of the country you live in, there are a number of different legal justifications FCTG relies upon in order to hold and use your personal data. When required under these privacy laws, at least one of the following justifications will apply:

- Where you have given your voluntary consent to us collecting/using your personal information.
- Where collecting/using your personal information is necessary for fulfilling a contract we have in place with you, such as your employment contract.
- Where FCTG needs to collect/use your personal information in order to meet our other legal obligations. Examples here include where FCTG needs your personal information under tax laws, health and safety obligations, and employment law requirements, to list a few.
- Where collecting/using your personal information is necessary to meet the legitimate business interests of FCTG.
- Where collecting/using your personal information is the necessary to protect your vital interests.

It is worth clarifying here that FCTG will rarely seek to rely upon, and obtain, your voluntary consent as the basis for holding/using your personal information, and wherever another option is available FCTG will use that option. There are two main reasons why FCTG has taken this position.

Firstly, it is poor practice to seek to rely upon consent in an employer-employee relationship given the power imbalance that exists between employers and employees. Consent is meant to be *voluntary*, but employees may feel they cannot refuse requests from their employers to provide their personal data, which undermines the whole concept of *voluntary* consent. Secondly, your continued employment in your role may require you to provide us or designated third parties your personal information, which does not reflect the idea of voluntary consent. Hence FCTG's position of relying upon other lawful mechanisms for collecting and using your personal information as an alternative where they exist. That being said, where there are no other viable options, and voluntary consent is relied upon for the collection of your personal data, it will occur in accordance with your local privacy laws which may provide you the right to withdraw that consent at any time.

In some circumstances, we may collect personal information from you which may be regarded as sensitive information under your local privacy laws. Depending upon your local privacy laws, sensitive personal information may include, amongst other things, your racial or ethnic origin, religious beliefs or affiliations, sexual orientation, biometric information, financial information and health information. We will only ever collect, hold and use your sensitive information in compliance with your local data protection laws.

We make every effort to maintain the accuracy of your personal information which we store and to ensure all your personal information is kept up to date. However, you can assist us with this considerably by promptly contacting us if there are changes to your personal information or if you become aware that we have inaccurate personal information relating to you.

4. What do we use your personal information for, and how long do we hold it for?

In this section we set out the different ways we use those categories of your personal information listed earlier in section 2. FCTG will update this Internal Privacy Notice should there be changes to the way your data is used, and make sure these changes comply with your local privacy laws.

Processing purposes	Data categories
Ensuring the security of our systems, networks, applications, and devices.	- Identifiers (online) - Work identifiers - Contact information (work) - Location information - Communication data - System & network generated data
Protecting against, deterring, detecting and investigating fraudulent, unauthorised or illegal activities	- Identifiers (offline) - Identifiers (online) - Work identifiers - Contact information (home) - Contact information (work) - Banking, payment card and tax information - Financial information - Human resource files (containing professional and employment-related information) - Location information - Biometric data - Performance data - Work history - Travel information - Communication data - System and network generated data - Training information - Customer/client interaction information
Ensuring the health and safety of staff while in the workplace or while travelling for work.	- Identifiers (offline) - Work identifiers - Contact information (home) - Contact information (work) - Emergency contact information - Medical and health & safety information (physical and mental) - Location information - Biometric data - Travel information
Maintaining accurate work history records of our employees.	- Identifiers (offline) - Identifiers (online) - Work identifiers - Contact information (home) - Contact information (work) - Government issued forms of identification - Banking, payment card and tax information - Pre-employment checks - Medical and health & safety information (physical and mental) - Financial information - Human resource files (containing professional and employment-related information) - Work history - Training information
Regulatory reporting and any other regulatory compliance requirements.	- Identifiers (offline) - Work identifiers - Contact information (home) - Contact information (work)

	- Government issued forms of identification - Banking, payment card and tax information - Medical and health & safety information (physical and mental) - Financial information - Diversity information - Training information
Developing and improving our products, services, systems and operational processes.	- Identifiers (online) - Work identifiers - Financial information - Location information - Performance data - Travel information - Communication data - System and network generated data - Customer/client interaction information - Employee survey responses
Quality and assurance activities in relation to the servicing of our customers, clients, other employees, or the public.	- Identifiers (online) - Work identifiers - Contact information (work) - Performance data - System and network generated data - Training information - Customer/client interaction information
Undertaking surveys and other collection mechanisms in order to meet specified business goals.	- Identifiers (offline) - Work identifiers - Employee survey responses
Training of staff.	- Identifiers (offline) - Work identifiers - Contact information (work) - Performance data - Work history - Communication data - System and network generated data - Training information - Customer/client interaction information - Employee survey responses
Assessing and managing the performance of all staff.	- Identifiers (offline) - Identifiers (online) - Work identifiers - Contact information (work) - Financial information - Location information - Performance data - Work history - Travel information - Communication data - System and network generated data - Training information - Customer/client interaction information
Creating, training, and/or utilising data-based models to facilitate the other processing purposes listed here. This includes the utilisation of third party pre-trained large-language models and generative AI applications.	- Identifiers (offline) - Identifiers (online) - Work identifiers - Financial information - Location information - Performance data - Work history - Travel information - Communication data - System and network generated data - Training information - Customer/client interaction information

To facilitate the provision of the services FCTG offer to customers and clients across all FCTG brands and business lines.	- Identifiers (offline) - Identifiers (online) - Work identifiers - Contact information (work) - Pre-employment checks - Location information - Performance data - Work history - Travel information - Communication data - System and network generated data - Training information - Customer/client interaction information
Ensuring FCTG is meeting its contractual obligations with corporate clients.	- Identifiers (offline) - Work identifiers - Pre-employment checks - Location information - Biometric data - Performance data - Work history - Travel information - Communication data - System and network generated data - Training information - Customer/client interaction information
Internal accounting, administration, management reporting, and business modelling.	- Identifiers (offline) - Work identifiers - Contact information (work) - Financial information - Location information - Performance data - Travel information - System and network generated data - Customer/client interaction information
Fulfilling our ongoing duty of care towards the individual on a day-to-day basis.	- Identifiers (offline) - Work identifiers - Contact information (home) - Contact information (work) - Emergency contact information - Medical and health & safety information (physical and mental) - Human resource files (containing professional and employment-related information) - Location information - Biometric data - Travel information - Communication data - Diversity information - Training information
Complying with a valid and authorised requests by law enforcement or government authorities or their agents, including court orders, or other valid legal processes and data requests.	Potentially all data held by FCTG. Scope per request is determined by the nature of the request and what is considered lawful to request under local legal regimes.
Meeting FCTG's legal compliance requirements, including but not limited to the fields of employment law, health and safety law, anti-bribery and corruption, equality laws, non-discrimination laws, etc.	- Identifiers (offline) - Identifiers (online) - Work identifiers - Family information - Contact information (home) - Contact information (work) - Government issued forms of identification - Banking, payment card and tax information - Emergency contact information

	- Medical and health & safety information (physical and mental) - Financial information - Human resource files (containing professional and employment-related information) - Performance data - Work history - Travel information - Communication data - System and network generated data - Diversity information - Training information - Customer/client interaction information
Providing internal corporate travel to FCTG employees.	- Identifiers (offline) - Work identifiers - Contact information (home) - Contact information (work) - Government issued forms of identification - Emergency contact information - Medical and health & safety information (physical and mental) - Location information - Travel information - Communication data
All payroll activities to ensure the correct payment of staff, commissions, taxes, benefits, etc.	- Identifiers (offline) - Work identifiers - Contact information (home) - Contact information (work) - Government issued forms of identification - Banking, payment card and tax information - Financial information - Human resource files (containing professional and employment-related information) - Location information - Performance data
Facilitating the employment of staff, including all pre-employment checks and collection of necessary data from employees/candidates.	- Identifiers (offline) - Contact information (home) - Government issued forms of identification - Banking, payment card and tax information - Pre-employment checks - Emergency contact information - Medical and health & safety information (physical and mental) - Location information - Diversity information - Employee survey responses
Controlling and monitoring access to properties, systems, networks, applications, data and devices.	- Identifiers (online) - Work identifiers - Location information - Biometric data - System and network generated data
Monitoring activities of employees within properties, systems, networks, applications, databases, files and devices	- Identifiers (online) - Work identifiers - Location information - Biometric data - Communication data - System and network generated data
Enforcing FCTG's legal rights and obligations.	This will vary on a case by case basis, but can potentially include any personal information held by FCTG.
Assessing and undertaking customer and employee subject access requests.	This will vary on a case by case basis, but can potentially include any personal information held by FCTG.

Measuring, recording, and benchmarking the performance of employees.	- Identifiers (offline) - Identifiers (online) - Work identifiers - Financial information - Location information - Biometric data - Performance data - Work history - Travel information - Communication data - System and network generated data - Customer/client interaction information
Performance management and disciplinary activities.	- Identifiers (offline) - Identifiers (online) - Work identifiers - Location information - Biometric data - Performance data - Work history - Travel information - Communication data - System and network generated data - Training information - Customer/client interaction information
Staff monitoring.	- Identifiers (offline) - Identifiers (online) - Work identifiers - Contact information (work) - Location information - Biometric data - Performance data - Travel information - Communication data - System and network generated data
Dispute resolution, whether in relation to external customer-facing activities or internal disputes between employees.	- Identifiers (offline) - Work identifiers - Human resource files (containing professional and employment-related information) - Location information - Biometric data - Performance data - Work history - Travel information - Communication data - System and network generated data - Training information - Customer/client interaction information
Provision of services, benefits, subsidies, assistance to employees.	- Identifiers (offline) - Identifiers (online) - Work identifiers - Contact information (home) - Contact information (work) - Government issued forms of identification - Banking, payment card and tax information - Financial information - Human resource files (containing professional and employment-related information) - Location information - Biometric data - Travel information - Communication data - Diversity information - Customer/client interaction information - Employee survey responses

For the retention of your personal information, we will retain your personal data for as long as it is necessary to fulfil the purposes for which it was collected. In addition, when we are under a legal obligation to retain elements of your personal information, FCTG will comply with any such obligations. We will delete your personal data, or anonymise that data (i.e., remove the ability for the data to be associated to you at which point that data is no longer considered your personal information), as soon as it is reasonable to assume that such retention no longer serves the purposes for which the personal data were collected, and are no longer necessary for legitimate legal or business purposes.

5. Is personal information disclosed to third parties?

Please note that FCTG does not, and will not, sell, rent out or trade the personal information of our employees. However, it is unavoidable that your personal information will be disclosed to third parties outside of FCTG as part of your employment by FCTG. We only disclose your personal information to the types of third parties set out below, and in accordance with your local data protection laws:

- Our independent contractors, suppliers and service providers. Some examples of these include the following:
    - suppliers of IT based solutions that assist us in providing products and services to you (such as any external data hosting providers we may use);
    - service providers (such as payroll, medical insurance, employee benefit schemes);
    - publishers, printers and distributors of personalised materials or materials sent directly to you;
    - organisers of FCTG events;
    - marketing, market research, research and analysis and communications agencies employed by FCTG for internal research;
    - mailing houses, freight services, courier services to send materials to you directly; and
    - external business advisers employed by FCTG (such as lawyers, accountants, auditors and recruitment consultants);
    - third party contractors engaged by FCTG to provide some service, the provision of which requires the processing of some of your personal information.
- FCTG's clients and customers where this is relevant to your role.
- FCTG's related entities and brands.
- Travel-related service providers when booking your business-mandated travel, such as travel wholesalers, tour operators, airlines, hotels, car rental companies, transfer handlers and other related service providers.
- Third parties to whom FCTG assign or novate any of our rights or obligations;
- Financial institutions such as banks, credit providers, issuers and payment service providers, when processing financial transactions, wages, etc.
- Your emergency contact (or a person who can verify to us that they have a relationship with you like a family member), where as a result of an emergency situation or similar unforeseen circumstances, in our opinion we need to contact this person on your behalf.
- Occupational health providers for the purpose of supporting you in your work and meeting our own legal obligations.
- Customs and immigration to comply with our legal obligations and any applicable customs/immigration requirements relating to your employment.
- Government agencies and public authorities to comply with our legal obligations and/or to comply with a valid and authorised request, including a court order or other valid legal process.
- National regulatory bodies and law enforcement officials and agencies, including to protect against fraud and for related security purposes;
- Enforcement agencies where we suspect that unlawful activity has been or may be engaged in and your personal information is a necessary part of our investigation or reporting of the matter.

- Our providers of systems, services, networks, applications, and databases.
- To external lawyers and advisers whether engaged by FCTG or not, to participate in the defence of a legal action against FCTG.
- Any circumstance other than those mentioned above, in terms of which FCTG may be obliged by any law, or a valid order of any court of competent jurisdiction or government authority acting with the powers granted to it in law, to disclose any personal information to any third party

As we discussed in section 1 *Background and Scope*, FCTG is a data controller and this Internal Privacy Notice describes how we process your personal information. We need you to be aware that when we transfer your personal information to the entities listed, they will either be processing this information under our control or they will be processing your personal information as an independent data controller, separate from FCTG's control. Where they are an independent controller, their privacy notice will apply and not FCTG's Internal Privacy Notice. Contact your local Privacy team and they will be able to assist you by identifying the exact role of each recipient (see section 14 below).

6. Is my personal information transferred overseas?

Yes. FCTG is a global organisation. Our IT systems, internal functions/departments, staff members and managers, can be located in any region or county globally. As a result, it is unavoidable that over the course of your employment your personal data will be processed outside of the country you normally live in.

Whenever we transfer your data overseas, FCTG ensures that all legal compliance requirements are met before any overseas transfer of your data occurs, and that the necessary protection measures are in place to make sure your data is protected regardless of where we process it.

(a) Our overseas related entities

FCTG operates a global business, with offices (or affiliated operations) in the following countries: Australia, New Zealand, Canada, United States, United Kingdom, South Africa, Hong Kong, India, China, Singapore, Japan, the United Arab Emirates, Kingdom of Saudi Arabia, Ireland, the Netherlands, Malaysia, Mexico, Germany, Norway, Sweden, Denmark, Finland, Spain, France and Switzerland.

(b) Booking overseas business travel

We are a global organisation, so depending on your role over the course of your employment within FCTG you may be required to travel outside of the country you live in. In order to book such travel we will need to provide certain elements of your personal information to the relevant overseas travel service providers.

(c) China cyber security law requirements

Personal information which is collected and generated within the territory of the People's Republic of China is stored within China's territory except for the following situations:

1. When we are lawfully able to transfer your personal data out of China.
2. We will transfer your personal information overseas in order to book overseas hotels, airlines, and travel related services or products.

For all international transfers of your personal data, FCTG ensures these occur in compliance with all local laws and that suitable safeguards are in place. If you have any specific questions about where or to whom your personal information will be sent, please refer to the "Feedback / Complaints / Subject Access Requests / Contacts" section below (section 14). Here you will find the right people internally to direct your questions to.

7. Security of information

Safeguarding and protecting the personal information entrusted to us by each of our employees is a responsibility we take incredibly seriously. This is why we continue to invest in a range of technical and organisational measures designed to ensure there exists an appropriate level of security to protect any personal information provided to us from accidental or unlawful access, misuse or destruction. We regularly review our security technologies as we strive to protect your personal information. We also actively destroy or de-identify your personal information once we no longer require it for our business purposes or to meet our own legal obligations.

It is also important for you to know that there are limits to what FCTG can control. Unfortunately, FCTG is not responsible for the actions or security controls of third party controllers we work with

and may provide your personal information to, or that they collect via their own websites or services. For example, when FCTG books staff travel for you the airlines and hotels used will process your personal information, however, FCTG is not responsible for the security controls of these airlines and hotels.

8. Your rights in relation to the personal information we collect

As an FCTG employee, depending upon where you are based you may have the right to make what is known as a Subject Access Request (SAR). Whether you have the ability to make a SAR, and exactly what you can request under a SAR, is determined by your local privacy laws. What is covered under a SAR can vary by country, but in many locations a SAR enables you to request one or more of the following actions/outcomes in relation to your personal information:

- you seek to either get access to, update, modify or fix, erase, object to, or obtain a copy of the personal information that FCTG holds on you; or
- you ask FCTG to restrict or stop us from using any of the personal information which we hold on you, including by withdrawing any voluntary consent you have previously given to the use of such information; or
- you request that we send a copy of your personal information to another entity.

You can make any of these requests by contacting us as set out in section 14 below, and we will acknowledge receipt of any request you make. SARs are governed by the different privacy laws of the country and/or state you live in, and we will always process your requests within the timeframes set by the privacy laws that apply to you.

While you may have a right to make a SAR under your local privacy laws, it will not always be possible to fulfil your requests. Often there are exclusions or restrictions set out within these same privacy laws that either prevent FCTG from fulfilling your request, or there are other factors we need to take into consideration before deciding how far we are able to respond. If we deny all or some part of your request, we will strive to provide you with written reasons as to why we are acting in this manner.

Please note that you may also have the right to lodge a complaint with a relevant supervisory authority.

If you have any questions regarding your right to lodge a SAR please reach out to your local data privacy team using the details set out in section 15 below. You can also use the online links in section 14 to lodge your SAR.

9. Singapore Requirements

This section pertains only to the processing of personal data by us that falls specifically within the scope of the Singapore Personal Data Protection Act ("PDPA").

Where voluntary consent to the processing of personal data has not been obtained, we will collect, use and disclose personal data pursuant to an exception under the PDPA or as required/authorised under any other written law.

Upon receipt of a written request to withdraw your voluntary consent, we may require reasonable time (depending on the complexity of the request and its impact on our relationship with you) for your request to be processed and for us to notify you of the consequences (including any legal consequences which may affect your rights and liabilities to us) of us completing this request. We will never delay our processing of such requests, and in any event will process them in accordance with the timelines set by the PDPA.

10. Social Media Integrations

Our websites and mobile applications may use social media features and widgets (such as "Like" and "Share" buttons/widgets) ("SM Features"). These are provided and operated by third party companies (e.g., Facebook) and either hosted by a third party or hosted directly on our website or mobile application. SM Features may collect information such as the page you are visiting on our website/mobile application, your IP address, and may set cookies to enable the SM Feature to function properly.

If you are logged into your account with the third party company, then the third party may be able to link information about your visit to and use of our website or mobile application to your social media account with them. Similarly, your interactions with the SM Features may be recorded by the third party. In addition, the third party company may send us information in line with their policies, such as your name, profile picture, gender, friend lists and any other information you have chosen

to make available, and we may share information with the third party company for the purposes of serving targeted marketing to you via the third party social media platform. You can manage the sharing of information and opt out from targeted marketing via your privacy settings for the third party social media platform.

Your interactions with these SM Features are governed by the privacy policy of the third party company providing them. For more information about the data practices of these third party companies, and to find out more about what personal information is collected about you and how the third party uses such personal information, please refer to their privacy policy directly.

11. IP addresses

When you access our devices, networks (whether through a device provided by FCTG or your own device), websites, use any of our desktop and/or mobile applications or open electronic correspondence or communications from us, our servers may record data regarding your device and the network you are using to connect with us, including your IP address. An IP address is a series of numbers which identify your computer, and which are generally assigned when you access the internet.

We may use IP addresses for system administration, investigation of security issues and compiling data regarding usage of our website and/or mobile applications. When this does occur, it will be done in accordance with the applicable Acceptable Use Policy. We may also link IP addresses to other personal information we hold about you and use it for the purposes described above (e.g., to link a user to their FCTG device).

12. Tracking Technologies / Cookies

We may use third party web analytics services on our websites and mobile apps, such as those listed in our Cookies Policy. The analytics providers that administer these services use technologies such as cookies and web beacons to help us analyse how visitors use our websites and apps.

For information regarding our use of cookies and tracking technologies, refer to our Cookies Policy on our website.

13. Linked Sites

Our websites may contain links to third party websites over which we have no control. We are not responsible for the privacy practices or the content of such websites. We encourage you to read the privacy policies of any linked third party websites you visit as their privacy policy and practices may differ from ours.

14. Feedback / Complaints / Subject Access Requests / Contacts

The Privacy team within FCTG does not only represent the business and our customers/clients, but is also here to protect, represent, and advocate for you, our FCTG employees. If you have any questions, complaints, or concerns about how FCTG uses your personal data, please contact us using the details below. Similarly, if you have any enquiries, comments or complaints about this Notice, please contact the privacy team in your region.

If you wish to make a Subject Access Request to inform us of a change or correction to your personal information, request a copy of the information we collect on you, request deletion of your information or would like to restrict the further processing of your data, please use the appropriate SAR link in the table below. We will respond to these requests within the time period required by the applicable jurisdiction.

Region / Business	Email	Postal Address	SAR Link
Africa	privacy@fctg.co.za	299 Pendoring street, Pendoring Office Park, Block 8, Johannesburg, 2195	Africa SAR Request
Americas	privacy@am.flightcentre.com	Chief Privacy Officer 5 Paragon Drive, Suite 200, Montvale, NJ 07645	AMER SAR Request
Asia	DPO@fcm.asia	Chief Privacy Officer 30 Cecil Street, #22-01/08 Prudential Tower, Singapore, 049712	Asia/ SAR Request
Australia	privacy@flightcentre.com.au	Chief Privacy Officer 275 Grey Street,	AU SAR Request

		South Brisbane, Queensland 4101	
Cross Hotels & Resorts	dataprotection@crosshotelsandresorts.com	Chief Privacy Officer 30 Cecil Street, #22-01/08 Prudential Tower, Singapore, 049712	Cross SAR Request
Discova	dataprotection@discova.com	Buffalo Tours (Singapore) Pte Ltd 50 Armenian Street, #04-04 Wilmer Place, Singapore 179938 *or* Olympus Tours, Yaxchilan SM 17 Mz 2 Lt 13, Cancun, Quintana Roo, Mexico	Discova SAR Request
Europe & Middle East	data.protection@flightcentre.co.uk	Chief Privacy Officer Flight Centre (UK) Limited 4th Floor, 120 The Broadway, Wimbledon, London, SW19 1RH	EME SAR Request
New Zealand	privacy@flightcentre.co.nz	Privacy Officer 124 Vincent Street, Auckland, 1010	NZ SAR Request

15. Other policies

You acknowledge that this Notice is subject to your local FCTG employment policies and handbooks which govern the terms of your employment and nothing in this Notice is intended to amend, vary, or change the terms of your employment.

16. Changes to our Notice

We may amend this Notice from time to time. If we make a change to the Notice, the revised version will be posted internally. We will communicate internally to notify you of any significant changes to our Notice and indicate at the end of the Notice when it was most recently updated. It is your responsibility, and we encourage you, to check this Notice from time to time in order to keep yourself familiarised with the content.

This Privacy Notice was last updated on 11 October 2023.