Compass Education

Privacy Policy

Update April 2018

1.0 Introduction

In this policy “we”, “us”, “the Company” refers to Compass Education Pty Ltd and Compass Education Holdings Limited, our group companies (including international distributors), our web site at http://*.compass.education (the “Site”, our “Websites”, the “platform”), and all related web sites, downloadable software, mobile applications (including tablet applications), and other services provided by us and on which a link to this Privacy Policy is displayed, and all other communications with individuals though from written or oral means, such as email or phone (collectively, together with the Site, our “Service”, our “Products”).

For most content within the Compass platform, we act as the data processor and provide services and online solutions to our clients, being the data controller (information owner).

This policy has been updated to provide further clarification on our privacy and data protection processes and ensure alignment with jurisdiction obligations, including the GDPR.

1.1 We are committed to ensuring the security of and safeguarding the privacy of our clients, our clients users and data and our end-users.

1.2 Our platform uses and requires the use of internet cookies which are necessary for the provision of our services. In the event

that cookies may be optional for a service, we may ask you for your consent to our use of cookies when you use that specific service for the first time.

1.3 Our platform incorporates privacy controls which affect how we will process personal data. Privacy controls vary across the platform, based on the module or service being used and settings that may be set by your platform administrator (data controller).

1.4 The data controller (information owner) is usually easily identifiable through our platform branding and labelling, however should you wish to confirm or clarify the data controller entity for your data and account, you may email legal@compass.edu.au. Emails requesting details of the data controller must include the URL of the service/portal you are using as well as your full name and account ID (username).

Definitions

“Care Providers” an individual, entity (association, non-incorporated, partnership or incorporated body) that has a duty of care over an individual.

“Client” means a customer of Compass (or a Compass related company).

“Client Data“ means personal data, reports, addresses, and other files, folders or documents in electronic form that a User or Client of the Service stores within the Service.

“Personal Data” means any information relating to an identified or identifiable natural person.

“Public Area” means the area of the Site that can be accessed both by Users and Visitors, without needing to needing to log in.

“Restricted Area” means the area of the Site that can be accessed only by Users, and where access requires logging in.

“User” means an employee, agent, student, parent, guardian or representative of a Client, who primarily uses the restricted areas of the Site for the purpose of accessing the Service in such capacity.

“Visitor” means an individual other than a User, who uses the public area, but has no access to the restricted areas of the Site or Service.

2.0 The information we collect

We collect different types of information from or through the Service. The legal basis for Compass' processing of personal data are primarily that the processing is necessary for providing the Service in accordance with Compass' Terms of Service and that the processing is carried out in the legitimate interests of our clients. We may also process additional data upon your consent, asking for it as appropriate.

2.1 User-provided Information. When you use the Service, as a User or as a Visitor, you may provide, and we may collect, display or update your Personal Data. Examples of Personal Data include but are not limited to name, email address, mailing address, mobile phone number, and credit card or other billing information. Personal Data also includes other information, such as geographic area or preferences, when any such information is linked to information that identifies a specific individual. You may provide us with Personal Data in various ways on the Service. For example, when you register for an Account, use the Service, post Client Data, interact with other users of the Service through communication or messaging capabilities, or contact us with customer service related requests.

2.2 Information Collected by Clients. A Client or User may store or upload into the platform. Compass does not necessarily hold a direct relationship with the individuals whose Personal Data it hosts as part of Client Data. Each Client is responsible for providing notice to its customers and third persons concerning the purpose for which Client collects their Personal Data and how this Personal Data is processed in or through the Service as part of Client Data.

2.3 "Automatically Collected" Information. When a User or Visitor uses the Service, we may automatically record certain information from the User's or Visitor's device by using various types of technology, including cookies, "clear gifs" or "web beacons." This "automatically collected" information may include IP address or other device address or ID, web browser and/or device type, the web pages or sites visited just before or just after using the Service, the pages or other content the User or Visitor views or interacts with on the Service, and the dates and times of the visit, access, or use of the Service. We also may use these technologies to collect information regarding a Visitor or User's interaction with email messages, such as whether the Visitor or User opens, clicks on, or forwards a message. This information is gathered from all Users and Visitors.

2.4 Integrated Services. You may be given the option to access or register for the Service through the use of your user name and passwords for certain services provided by third parties (each, an "Integrated Service"), such as through the use of your Google account, authentication provider, or otherwise have the option to authorise an Integrated Service to provide Personal Data or other

information to us. By authorising us to connect with an Integrated Service, you authorise us to access and store your name, email address(es), date of birth, gender, current city, profile picture URL, and other information that the Integrated Service makes available to us, and to use and disclose it in accordance with this Policy. You should check your privacy settings on each Integrated Service to understand what information that Integrated Service makes available to us, and make changes as appropriate. Please review each Integrated Service's terms of use and privacy policies carefully before using their services and connecting to our Service.

2.5 Location Information. When accessing our service or installing our applications we may collect and process information about your actual location. We may use various technologies to determine location including IP addresses, GPS and other technologies including iBeacons/bluetooth or WiFi access points. When we have location information, we use this to tailor our service and platform to you, assist in jurisdiction compliance, trigger authentication confirmation, provide extended user validation, allow extended features (such as school arrival/departure/visitor check in), allow excursion tracking. Device based location services can be managed directly through your device.

2.6 Financial information. We may collect financial information related to an individual such as bank or credit card details used to transact with us and other information that allows us to transact with the individual and/or provide them with our services. We maintain this information in alignment with our PCI-DSS obligations. This information is shared with financial institutions (including banks and schemes) for the purpose of providing the service and to ensuring security and data protection compliance.

We may offer wallet services, which allow a user to link their credit card details in our service. In the event details are linked, we do so using a form of tokenisation. We offer tokenisation to assist our users, removing the need to re-enter credit card details – should they choose.

Tokenisation does not store your credit card details with us, instead we send these details to our secure banking partner, storing only a key in our system which allows us to forward this key and an amount to our banking partner in the future. In addition to this key, we may also store some identifying information about the card, to assist you in determining which card is linked. This may include the expiry date, card type and either the first and/or last few digits of the card.

The PCI DSS is a set of rules created by the Payment Card Industry Security Standards Council to encourage the broad adoption of consistent data security measures around the world.

More information about this standard can be found at www.pcisecuritystandards.org.

2.7 Sensitive Information
Sensitive information means information or an opinion about an individual's –

(i) racial or ethnic origin; or
(ii) political opinions; or
(iii) membership of a political association; or
(iv) religious beliefs or affiliations; or
(v) philosophical beliefs; or
(vi) membership of a professional or trade association; or
(vii) membership of a trade union; or
(viii) sexual preferences or practices; or
(ix) criminal record

While we try to minimise holding sensitive information, there are circumstances where we do hold these sensitive personal details. For example, we may record information relating to an individual's racial or ethnic origin for the purposes of providing our clients with reporting for relevant funding, welfare or educational services.

Medical information may be recorded and published in our systems to assist in preventing and/or lessening a serious and imminent threat to life and/or the health of an individual.

2.8 Unique Identifiers
Users are assigned unique identifiers on a per user basis for the purpose of providing consolidated, relevant data to the user. As our services are an enterprise solution, unique identifiers, created by our systems, are unique across our platform.

Our clients may choose to include unique identifiers, such as state, federal, international or school identifiers within our system for the purposes of meeting government reporting obligations. Often this is required to enable the organisation to carry out its functions efficiently and ensure compliance.

2.9 Biometric Data
Our clients may choose to enable the use of biometric technologies to assist in rapid identification and confirmation of a user's identity. Given the fact that biometric finger technology is relatively new we have included additional information in this area. Biometric verification may be used for a number of school related end user services, such as rapid verification of registered users, including staff, students, visitors or contractors for the provision of/access to restricted, user specific electronic tasks.

These services may include functionality such as:

- Visitor sign-in

- Class/Schedule lookup
- Password reset
- Late sign in
- Early departure
- Print/Fund top-up
- Canteen purchases

As biometric verification cannot be guaranteed to be 100% accurate, other verification steps may also be included, to confirm the user's identity.

Biometric finger-scan data collection is conducted by placing a finger on the 'finger-scanning' device on the relevant unit or computer.

Importantly, we do not store a copy of the user's fingerprint, instead we follow a process called finger-scanning, which involves hashing extracted features of the finger, to enable a 'best guess' comparison. We are unable to, and understand it is unlikely that one could, construct a fingerprint or replicate a copy of a user's fingerprint from a hashed feature extract of a finger-scan. Finger-scan data is stored in alignment with our Protection of data provision.

We follow the following process when registering a user's finger-scan. This process provides an indicative process flow that may vary slightly between devices.

Step 1 – Image capture (held in RAM based, non-permanent memory)
Step 2 – Best image selection (quality of images, up to 5 analysed for 'best capture')
Step 3 – Image optimisation, contract and noise reduction applied to image
Step 4 – Feature analysis and extraction
Step 5 – Hash template created (Finger-scan data)
Step 6 – Hash template stored (Finger-scan data)
Step 7 – Image discarded

We follow the following process when confirming a user's identity.

Step 1 – Image capture (held in RAM based, non-permanent memory)
Step 2 – Image optimisation, contract and noise reduction applied to image
Step 3 – Feature analysis and extraction
Step 4 – Live hash template created (Finger-scan data)
Step 5 – Image discarded
Step 6 – Comparison and matching between stored templates and live hash
Step 7 – Template matching score (with variance tolerance)

Given the nature of the biometric data stored, it is not practical to provide this in a human readable format. Accordingly, requests for copies of this data will be denied. However, biometric data will be removed from our services, including end-point devices, upon request. Further, this data is managed in alignment with our Destruction and retention of data provision.

2.10 Information from Other Sources. We may obtain information, including Personal Data, from third parties and sources other than the Service, such as our partners, advertisers, credit rating agencies, and Integrated Services (including but not limited to canteen, printing, postage, library and education service providers).

If we combine or associate information from other sources with Personal Data that we collect through the Service, we will treat the combined information as Personal Data in accordance with this Policy.

3.0 How we use the information we collect

We use the information that we collect in a variety of ways in providing the Service and operating our business, including the following:

3.1 Operations
We use the information – other than Client Data - to operate, maintain, enhance and provide all features of the Service, to provide the services and information that you request, to respond to comments and questions and to provide support to users of the Service. We process Client Data solely in accordance with the directions provided by the applicable Client or User.

3.2 Improvements
We use the information to understand and analyse the usage trends and preferences of our Visitors and Users, to improve the Service, and to develop new products, services, feature, and functionality.

3.3 Communications
We may use a Visitor's or User's email address or other information to contact that Visitor or User (i) for administrative purposes such as customer service, to address intellectual property infringement, right of privacy violations or defamation issues related to the Client Data or Personal Data posted on the Service or (ii) with updates on promotions and events, relating to products and services offered by us, our clients and by third parties we work with.

3.4 Cookies and Tracking Technologies

We use automatically collected information and other information collected on the Service through cookies and similar technologies to: (i) personalise our Service, such as remembering a User's or Visitor's information so that the User or Visitor will not have to re-enter it during a visit or on subsequent visits; (ii) provide customised content, client related advertisements and information; (iii) monitor and analyse the effectiveness of Service; (iv) monitor aggregate site usage metrics such as total number of visitors and pages viewed; and (v) track your entries, submissions, and status in any promotions or other activities on the Service. You can obtain more information about our use of Cookies in our Cookie Policy.

3.5 Electronic Health Records
We collect and manage electronic health records of users to assist our clients in the management their duty of care and enrolment obligations.
These records may be updated, viewed or removed by our clients with a duty of care over the individual (Care Providers).

3.6 Analytics
We use Google Analytics to measure and evaluate access to and traffic across the Site, and may create user navigation reports for our Site administrators and clients. Google operates independently from us and has its own privacy policy, which we strongly suggest you review. Google may use the information collected through Google Analytics to evaluate Users' and Visitors' activity on our Site. For more information, see Google Analytics Privacy and Data Sharing.

We take measures to protect the technical information collected by our use of Google Analytics. The data collected will only be used on a need to know basis to resolve technical issues, administer the Site, undertake or assist in security audits and identify visitor preferences.

4.0 Providing your personal data to others

4.1 We may disclose your personal data to any member of our group of companies (this means our subsidiaries, our ultimate holding company and all its subsidiaries, and/or any registered and approved franchisee companies of our holding company and its subsidiaries) insofar as reasonably necessary for the purposes, and on the legal bases, set out in this policy.

4.2 We may disclose your personal data to our insurers and/or professional advisers insofar as reasonably necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, obtaining professional advice, or the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

4.3 Financial transactions relating to services may be handled by our payment services providers. We will share transaction data with our payment services providers only to the extent necessary for the purposes of processing your payments, card tokenisation, refunding such payments and dealing with complaints and queries relating to such payments and refunds.

4.4 In addition to the specific disclosures of personal data set out in this Section 4, we may disclose your personal data where such disclosure is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person. We may also disclose your personal data where such disclosure is necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

4.5 Depending on your school, state and/or country, we may provide integrated extension services. These may include but are not limited to engaged third-party school providers of your school. For example: 1. We may provide integrated solutions to your schools approved School Photography company, to facilitate student and staff photos and/or ordering. 2. We may provide integration with other school approved solution such as Google, Office 365 or other online services.

4.6 You may choose to share your information with other third party providers, to enabled extended services such as, but not limited to state or council library integrations or other third party service integrators. In tapping your identity card or logging into a third party's systems, with your Compass credentials, you understand and agree, we may share your information with that provider. Where possible and appropriate, we will prompt you ahead of providing these details.

5.0 International transfers of your personal data

5.1 In this section, we provide information about the circumstances in which your personal data may be transferred to countries outside Australia.

5.2 **Australian Clients -** We do not host personally identifiable client data from our service outside of Australia.

5.3 **European Economic Area -** For clients based in the European Union transfers to Australia are protected by appropriate safeguards. We adhere to the obligations from Directive 95/46/EC of the European Parliament and of the Council and will provide our EU Compass Online Services Data Processing Agreement. To

request a copy of this agreement, you must be a client (school or incorporated body) registered with Compass Education Holdings Limited (Ireland) and should email legal@compass.education

5.4 **GDPR** applies to all EU data subjects so will apply to all companies and organisations who have EU citizens as part of their business or organization. GDPR will apply to all companies processing the personal data of subjects residing in the European Union, regardless of the company's location.

5.5 The hosting facilities for our website are situated in Australia and are located in an ISO27001 certified data centre.

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

5.7 In some circumstances we may limit access to information or our services from locations or services we consider to be high risk, these include but are not limited to VPN services.

6.0 Notice to End Users

Many of our products are intended for use by education organisations. Where the Services are made available to you through an organisation (e.g. your school or government), that organisation is the administrator of the Services and is responsible for the accounts and/or Service sites over which it has control. If this is the case, please direct your data privacy questions to your administrator, as your use of the Services is subject to that organisation's policies. We are not responsible for the privacy or security practices of an administrator's organisation, which may be different than this policy.

7.0 Changes

Our Privacy Policy may change from time to time. We will post any Privacy Policy changes on this page.

8. Contact Information

For more information on the management of privacy and data, please contact our privacy officer by post or email.

Postal contact information (Australia/Global)
Compass Education Pty Ltd
Privacy Officer
PO BOX 366
BALWYN NORTH, VIC 3104
AUSTRALIA

Postal contact information (European Union)
Compass Education Limited
Privacy Officer
Office 29, Clifton House
Fitzwilliam Street
Lower Dublin 2
IRELAND

Email contact information
Compass Education
Privacy Officer
legal@compass.education