Personal Data Privacy Policy

REACH Boarding School System including REACH BioPad.
(Touchline Connect Pty Ltd)

Last updated: 11 Nov, 2019
Version: A191111

This statement outlines the Personal Data Privacy Policy for the REACH Boarding School System (REACH) and REACH BioPad products developed and marketed by Touchline Connect Pty Ltd (Touchline Connect). It relates to the management of personal, private and sensitive information provided to or collected by the REACH and Touchline Connect as the vendor of the system and hardware operation. It applies to all of REACH's applications on web, mobile app and BioPad devices.

Touchline Connect may from time to time review and update this Privacy Policy to take account of new laws and technology, changes to the operations and practices and to make sure it remains appropriate to the changing school environment.

Touchline Connect is committed to protecting the privacy of all personal information that we collect and use in the operation of REACH. This Privacy Policy embodies this commitment and applies to personal information collected by Touchline Connect and its contractors and agents.

All personal information collected by Touchline Connect is, in all circumstances, protected by the relevant personal data privacy laws governing the various regional jurisdictions in which REACH operates. This policy takes into consideration all of the sovereign jurisdictons where REACH operates and sets the framework for our compliance to those regulations.

Sections

1) Collection of Personal Information

The type of information that Touchline Connect receives and holds, includes (but is not limited to) personal information, including sensitive information about:

- Students and parents and/or guardians ("Parents") and hosts before and during the course of a student's enrolment.
- Staff and other people who come into contact with the School for the management of School or Boarding House activities.
- Student medical records collected by the school and shared with or stored in REACH.
- Personal biometric fingerprint data in the form of unique digital binary codes converted from fingerprint images provided and approved by individuals using the REACH BioPad.

Personal Information about Parents, Students and Guardians

Touchline Connect will collect personal information about an individual from schools who use REACH. Parents and students will also have a capacity to update that information from time to time with secure, direct access to REACH and REACH BioPad.

Personal Information about School Staff and other third parties

Touchline Connect will collect personal information about an individual staff member or third party associated with the school or boarding house from schools who use REACH. These individuals will have the ability to update that information from time to time with secure, direct access to REACH.

We may also collect and use Personal Information from individuals where they provide that information in forms provided on our website, in phone conversations or email messages with REACH representatives. We may also collect and use Personal Information about individuals that is publicy available for the purpose of a legitimate interest in REACH.

Photographs

Touchline Connect will, as part of the activities of REACH, utilise photographs of individuals provided by the school or by the individual themselves for user and system identification purposes. Photographs of school activities, staff, students and other personnel may be posted on REACH by authorised school administration staff for internal use and promotional use by the school.

Touchline Connect will not use any photograph provided by the school for anything other than its intended purpose without knowledge and consent from the individual or individuals identified in the photograph.

Biometric Fingerprints

When implemented, the REACH BioPad captures images and measurements of fingerprints to extract unique biometric data of individuals in the REACH ecosystem. It uses a complex set of algorithms to identify and apply unique, minute measurements into an encrypted binary number template and no fingerprint images are retained in REACH.

Collection & Processing personal data of individuals under 18 years old

Personal information for children under the age of 18 may be uploaded into REACH by customers using REACH services where the customer is data controller and REACH is the data processor. The customer is responsible for ensuring that disclosing such information is done in accordance to applicable law, legal processes and regulations. For example, obtaining consent from their parents or legal guardians if applicable under the GDPR. REACH will not control such information and will act only as a procesor of this data.

2) Data Storage

REACH User Portals and applications that are cloud hosted are contained in secure data centres that physically reside in servers provided secured by the Google Cloud Platform which is ISO 27001, ISO 27017 and ISO 27018 certified for cloud based data security. Primary storage locations for REACH portals are in Australia, USA, UK and Singapore and Hong Kong. If you require more information regarding the specific server and hosting details for your school, please contact us.

Biometric Fingerprint Data

Biometric Fingerprint images are not stored in REACH BioPads or on REACH data servers. Each fingerprint image is immediately converted to a unique binary number template and the binary number is stored as an identifier for an individual user's profile in REACH. At no time are fingerprint images stored in REACH. The the unique binary numbers are created by and readable to only by the specific fingerprint reader and unique image conversion algorithm that is provided by REACH.

3) Use of personal information provided

The primary purpose of collection of personal information of students, parents, guardians, hosts and school staff is to enable REACH to provide an activity management system which assists schools to manage their duty of care for school and boarding house activities. This data is maintained in a secure environment with multi-layered security protocols for data protection.

Access to this data is limited to authorised school personnel and to individuals whose personal data is on the system.

An individual's access to personal data is restricted by security protocols to their own information or information relating to individuals that the school has formally associated them with on REACH.

The purposes for which Touchline Connect uses the personal information of students, parents, guardians and staff include:

- Keeping Parents and staff informed about matters related to a student's activities in the School and Boarding House, through correspondence, news alerts and activity notifications, and
- Satisfying the School's legal obligations and allowing the School to discharge its duty of care, and
- Providing user identity verification for access to and utilisation of REACH modules and activities.

Personal information collected by Touchline Connect will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless agreed otherwise, or where the use or disclosure of that personal information is allowed or required by law.

Images of individuals

Images of the School's students, staff, parents, guardians and other visitors may be used in various instances by authorised school administration staff using REACH. Only authenticated users may insert photographs into the REACH system. Touchline Connect will not use any photographs or images provided by the School without consent from the individual or individuals identified in the photograph or image.

Biometric Fingerprint Data

Biometric Fingerprint Data is used for the sole purpose of user identity verification to enable access to various application activities within the REACH ecosystem only. Touchline Connect will not use any Biometric Fingerprint Data outside of the REACH ecosystem or for any purpose other than to verify an individual user's identity.

4) Disclosure of personal information

Touchline Connect will not share personal information held about an individual with any third party without a school's approval of the sharing of data with that third party except in the following instances:

- REACH may transfer personal information via direct data connections with a school 's existing database or other computer systems for the purpose of maintaining accurate and co-ordinated school records.
- The disclosure is required or authorised by or under law.
- The disclosure is reasonably necessary for the enforcement of the criminal law.
- We have reasonable grounds to determine that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another individual.

5) Protection of personal information

Touchline Connect manages the security of personal information with physical, electronic and procedural safeguards.

We urge individuals to take every precaution to protect their personal data when connecting to REACH by regularly changing passwords, using alpha-numeric combinations, not sharing usernames or passwords with other users (including family members) and ensuring that a secure browser is used to access REACH.

Touchline Connect has in place a number of data protection steps to protect the personal information that is contained in REACH. These include:

- Servers that are connected to UPS power and have RAID disk arrays for greater reliability.
- Servers that are fully locked down, running only essential services, with CISCO firewalls and CISCO routers used to secure data.
- Servers backed up daily and tapes stored in a fireproof safe.
- Servers housed in premises on a secure floor with 24 hour PIN access.

Biometric Fingerprint images are not stored in REACH. An encrypted binary template (i.e. measurements taking from the fingerprints captured) is created from fingerprint images and used to establish the characteristic for each unique identity and this is verified when replica binary prints are identified. Importantly, this encrypted binary template is only usable in the REACH system.

Checking and updating personal information held by REACH

In accordance with the Privacy Act 1988, an individual has the right to obtain access to any personal information which REACH holds about them and to advise of any perceived inaccuracy. There are some exceptions to this right, set out in the Act for minors. Students will generally have access to their personal information through their Parents or Guardians.

Other individuals with personal data on the REACH system and who are approved by the school 's system administrator may have access to their own personal data and in some cases to other individuals with whom the school administrator has associated them in REACH.

6) Matters relating to use of the REACH Cloud-portal and REACH website Information Collected

When you view and use the REACH web portal or the REACH website the following information is collected for statistical purposes:

- The Internet Protocol (IP) address of the machine from which you are connecting. Your top level domain name (for example .com, .gov, .au, .uk etc).
- The date and time of your visit to the site.
- The pages that you accessed and any documents downloaded.
- The previous site you had visited.
- The type of browser you are using and the operating system that it runs on.

Access to information collected

No identifying data is provided to any parties other than the relevant portal administrators and authorised operators. In the event of an investigation where a law enforcement agency may exercise a warrant to inspect our internet web server logs, then access to information collected will be provided in accordance with any legal requirements.

Use of information collected

Email addresses and phone numbers collected will only be used for the purpose for which they have been provided to us by the school or by the individual. They will not be added to marketing or mailing lists or used for any other purpose without your consent other than for the provision of information relevant to the operation of the REACH system.

Cookies

The REACH web portal and the REACH website use "Session" cookies to aid in the ease of browsing through the site. In this situation, the cookie identifies the browser, not the individual. No personal information is stored within the cookies of Touchline Connect.

You can manually disable cookies at any time. Simply check your web browser's "Help" function to find out how to disable cookies in your web browser. Disabling cookies will not impact your ability to access the REACH web portal or the REACH website.

Google Analytics

REACH User Portals are not monitored using any external tracking programs. In portal, analytics are utilised to monitor user traffic flows and movements however all data is maintained within our own server network and the data is not shared with any third party.

Google Analytics is used by Touchline Connect to collect website visitor information for our various websites. This includes the REACH website but it does not include any REACH User Portals.

Google Analytics uses first-party cookies and JavaScript code to help analyse how users use the site. It anonymously tracks how visitors to these sites interact with the websites. The information generated by the cookies about your use of the website (including your IP address) will be transmitted to and stored by Google on servers in the United States. Google will use this information for the purposes of compiling reports on website activity and providing other services relating to website activity and internet usage. You may refuse the use of cookies by selecting the appropriate settings on your browser.

7) Data Retention

If a customer ceases to use the REACH system then the customer will be provided with their current and historic REACH database and backup files in compressed format. The customer may be required to hold this data for a minimum specified period however all personal information relating to individual students, parents, guardians, hosts and staff these records will be stored in backup files only.

Sensitive information removal

Information classified as “sensitive information” by the Privacy Act 1988 includes student medical records and fingerprint biometric data. This data is treated more diligently than general personal data. Whereas personal data may be contained and hidden from view and access to system users when an individual is deleted (hidden) or retired (graduated) from the REACH system, sensitive information will be removed so that it is no longer contained in the REACH system within seven (7) days of an individual being deleted (hidden) or retired (graduated) from a customer’s REACH portal.

Once removed from a customer’s REACH portal, any sensitive data relating to an individual will remain only in compressed and encrypted backup files for a customer’s REACH portal where it is retained as relevant, historic data records. The sensitive data will not be accessible from any live REACH portals and if the customer is no longer using REACH then all encrypted backup files will be removed entirely from the REACH storage environment and provided to the customer for future storage or destruction.

8) Complaints

If any person believes that we may have breached their privacy, they may contact us to make a complaint using the contact details below. In order to ensure that we fully understand the nature of any complaint and the outcome they may be seeking, we prefer that all privacy complaints are made in writing.

Touchline Connect undertakes to assess and resolve all privacy complaints diligently and in a timely manner.

Contact Us

If you have any enquiries or complaints about privacy, or if you wish to access or correct your personal information, please contact Mr Garry Jowett on Ph: 1300 215199 or on email at garry@touchline.com

Changes to this privacy policy

Please note that the privacy policy may change from time to time.