BioPad

Fingerprint Biometrics

A guide to fingerprint use and data security with REACH BioPad.

REACH
Boarding School System

The purpose of this document is to provide information for schools, their staff and their boarding community with regards to the utilisation of fingerprint biometric data at schools implementing the REACH BioPad.

At the outset, it must be acknowledged that your school, and REACH as a vendor, are subject to the provisions of the Privacy Act 1988. Any changes to this regulation in the future, including the Australian Privacy Principles which set out how entities must handle, use and manage personal information, will supersede any of the information provided in this document.

REACH BioPad

The REACH BioPad is a device that is used with the REACH Boarding School System. It allows schools to:

- Track the movement of students as they move to and from various locations that the school tracks. This includes approved leave departures and returns, in addition to other on and off campus locations that the school tracks. Knowing where a student is at any time is an important duty of care requirement for the school and allows them to know, at any time, where students are in case there is an emergency.

- Conduct Automated Rollcalls where student register their presence at a time and place (eg: breakfast rollcall, weekend mid-day campus check)

- Capture and verify host and parent identities when collecting students for off campus leave events. This includes the ability to capture signatures and/or photographs of the host that is collecting the student for a leave event.

The REACH BioPad is able to use several methods of authentication in order to verify a user's identity including;

1. PIN number
2. RFID card read
3. NFC Device read
4. Biometric Fingerprint
5. Biometric Facial Recognition

Note: Biometric Facial Recognition is not activated in the REACH BioPad at the time of writing this document so this document is concerned specifically with providing parents, guardians, hosts and staff with information and guidelines on policies and procedures for the collection, storage, utilisation and storage of Biometric Fingerprint Data by REACH BioPad.

What are Biometrics?

Biometrics is data that measures personal information about an individual's physical or behavioural characteristics in order to verify their unique identity. It covers a wide range of personal characteristics including fingerprint identification, iris and retina scanning, face recognition, vein geometry and voice recognition.

The use of biometrics is becoming increasingly common in both public and private sectors. It is also now commonly used as a personal device security mechanism (eg: mobile phone or PC).

REACH BioPad and the REACH Boarding School System is restricted to using fingerprint biometrics information only. Any photographs taken by the REACH BioPad may be stored for event record purposes only and they are not used, stored or recorded for biometric facial recognition purposes.

Why use Biometrics?

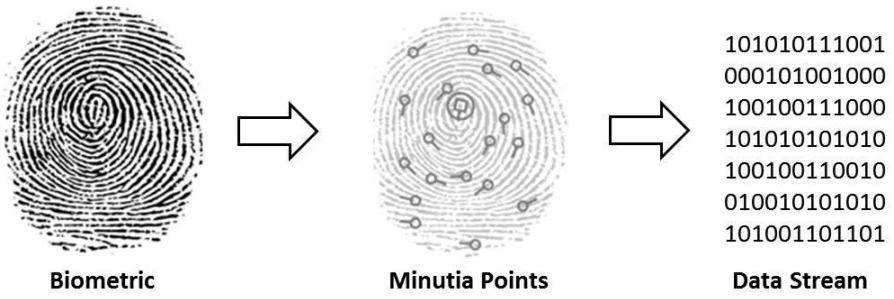
Biometrics are suited to all applications where the accurate identification of an individual is essential. Its utilisation in school administration has grown globally in the past decade because it provides an ideal solution for school administrators in their effort to identify students, provide accurate and auditable student records and provide a safer and more secure environment for students, teachers and staff.

Biometrics provides a level of certainty that is not possible with other methods of identification verification. Student Identity Cards are regularly forgotten, lost, mutilated and shared; PINs and Passwords are easily forgotten, swapped or stolen. These current methods of identity verification do not offer a level of assurance that is indisputable.

By using biometrics for identification, the problems and costs associated with the current methods can be avoided and new standards of accountability can be put into place.

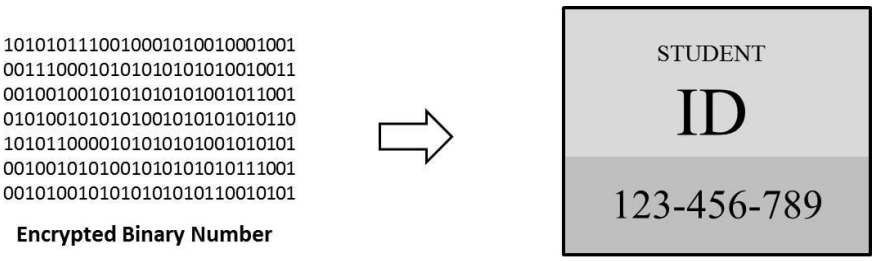
How we record Biometric information

REACH BioPad captures images and measurements of fingerprints to extract unique biometric data. It uses a complex set of algorithms to identify and apply unique minutiae measurements into an encrypted binary number template.



An important distinction in the procedure for fingerprint data management using REACH is that an image of the fingerprint is never stored by the REACH BioPad or the REACH Boarding School System itself.

An encrypted binary template (i.e. measurements taking from the fingerprints captured) is created 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.



How REACH BioPad differs from law enforcement fingerprinting

There are several significant differences between finger printing law enforcement applications and finger scanning identification methods that are used by the REACH BioPad.

Finger printing in the law enforcement context captures and stores rolled images of fingers. Rolled images capture unique identifying points on the entire finger surface in order to collect the maximum number of unique identifying points. Finger scanning uses flat images of a

fingerprint to create binary templates. Flat images reveal the centre of the finger and require only a minimum of unique identifying points in order to generate a digital interpretation and no fingerprint images are ever stored. The purpose of the REACH BioPad scanning process is to identify and recognise a person that is already enrolled in the software.

Data Privacy for Australian Schools

In considering personal data privacy, it is important to recognise that Biometrics are not the enemy of privacy. In fact, in many instances, the use of biometrics is privacy and security enhancing.

At all times, your school and the REACH Boarding System are bound by the provisions of the *Privacy Act 1988*, including the Australian Privacy Principles (APPs). This is regarding all private information collected and used, including any biometric data. An outline of the APPs is provided in Appendix 2 of this document.

The APPs set out standards, rights and obligations for how we handle and maintain people's personal information. This includes how we collect, store, use, disclose, quality assure and secure personal information, as well as an individual's rights to access or correct their personal information. A full version of the Personal Data Privacy Policy for REACH Boarding (Touchline Connect Pty Ltd) is provided as Appendix 1 to this document.

Biometric information that is used for the purpose of automated biometric verification or biometric identification is considered to be sensitive information under the Privacy Act 1988.

Sensitive Information

'Sensitive information' is specifically defined under the Privacy Act and it includes information about an individual's racial or ethnic origin, political opinions, professional, political or religious affiliations or memberships, sexual orientation or practices, criminal record, health, genetics and/or biometrics.

Sensitive information is afforded a higher level of privacy protection under the Privacy Act than other personal information. This recognises that the inappropriate handling of sensitive information can have adverse consequences for an individual or those associated with the individual.

'Sensitive information' is subject to a higher level of privacy protection than other 'personal information' in the following ways:

1. 'Sensitive information' may only be collected with consent, except in specified circumstances. Consent is generally not required to collect 'personal information' that is not 'sensitive information.
2. 'Sensitive information' must not be used or disclosed for a secondary purpose unless the secondary purpose is directly related to the primary purpose of collection and within the reasonable expectations of the individual.

3. 'Sensitive information' cannot be used for the secondary purpose of direct marketing.

4. 'Sensitive information' cannot be shared by 'related bodies corporate' in the same way that they may share other 'personal information'.

Policy Guidelines & Recommendations for Australian Schools using REACH biometric data

The following are guidelines for schools when implementing the REACH BioPad for the collection and use of biometric data.

(Note: The REACH Biopad can also be used without fingerprint implementation using RFID, NFC or PIN as identity verification procedures).

If your school currently collects medical information about your students then it will already be required to meet these guidelines for the collection, storage, use and retention of medical information which is also considered to be 'sensitive information' under the Privacy Act 1988.

1) Review your current Privacy Policy
Review and update your school's personal data privacy policy to ensure that it includes reference to and provisions for the collection, use and storage of personal biometric data.

REACH Response: REACH Boarding (Touchline Connect Pty Ltd) provides an updated Personal Data Privacy Policy which specifically addresses sensitive information including medical and biometric data for individuals using the REACH Boarding System.

2) Notification & Consent to all Users
Notification and consent requests must be provided to all users who are asked to participate in the biometric fingerprint identification system. This includes students, parents, hosts and staff. In particular:

- Parent/s must be informed by the school that they are using a biometric system and the school must gain written consent from the parent/s to take and process their child's biometric data. Parents may withdraw their consent at any time.

- Regardless of the consent given by parents, students must be given the ability to personally determine whether a school collects and processes their biometric data. If a student elects not to participate in the biometric system, the school must provide an alternative and must not withhold any services from the student that are available through the biometric system. A student may withdraw their consent at any time.

REACH Response: REACH Boarding (Touchline Connect Pty Ltd) provides consent form templates for intended users of REACH BioPad.

3) Control Biometric Data Use

Provide clear guidelines to your parent, student, host and staff users outlining how and when they will be asked to provide and use biometric fingerprint authentication.

- Do not permit function creep for the use of biometric data collected by the REACH BioPad without the knowledge and consent of your user population.

- Personal biometric data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with purpose specified in your request for consent form except with the consent of the data subject or by the authority of the law.

<u>REACH Response:</u> REACH Boarding provides clear details of intended use for biometric data collected and utilised using the REACH BioPad or the REACH Boarding System in the Consent Request Form template. These details are replicated in the Personal Data Privacy Policy of Touchline Connect Pty Ltd ensuring they are implemented regardless of whether your school uses the REACH template with your user community.

4) Control Data Retention

Implement diligent biometric data retention and destruction procedures. Upon request from the biometric subject or departure from your school, the biometric data should be diligently removed from all devices and storage media.

<u>REACH Response:</u> Importantly, no fingerprint images are ever stored in the REACH system, only digital interpretations as binary numbers are stored in the personal records of users. REACH Boarding provides automated deletion of user identifiers when a user is removed from use in the REACH Boarding System. "Removed from REACH use" means where an individual is deleted (hidden) or retired (graduated) from the REACH System. In any case, user identifiers are deleted within seven (7) days of a user being deleted (hidden) or retired (graduated) from the REACH System. These details are set out in the Personal Data Privacy Policy of Touchline Connect Pty Ltd

5) Update Provider Agreements

Update your vendor agreements that deal with biometric data, or have access to systems with biometric data.

<u>REACH Response:</u> If you use REACH BioPad and associated biometric data then your REACH Service Level Agreement will include details outlining the policies and procedures required and implemented by REACH for the collection, storage, utilisation and retention of personal biometric data for all relevant users.

Sample Notification and Request Form

Dear Parent,

For the REACH Boarding School System we require the consent of at least one parent in order that the biometric information of your child can be processed.

Please be assured that this information remains stored within and is used solely by the REACH Boarding System. The biometric information that will be stored is a mathematical algorithm of your child's fingerprint and not the actual finger print image itself. This algorithm is readable only within the REACH Boarding System. It will be used to authenticate your child's identity for sign in and sign out to locations in the REACH System and for some Roll Call activities.

If you choose not to have your child registered, the school will provide alternative methods of identification such as a four digit PIN code.

The preference of the school is to use biometrics because this is the most secure and accurate authentication method for identification verification. We appreciate your co-operation with regards to this matter.

Could you please therefore complete and sign the form below and return to the Boarding House Administration Office.

OPT IN FORM TO PARENTS

I confirm that I wish my child _*student name*_____ TO BE/NOT TO BE (please delete where applicable) registered on the school's REACH BioPad Biometric System with immediate effect.

I understand that I may withdraw my child's registration at any time in writing.

_____

Parent Name

Date: _____

Questions & Answers for Parents and students about the use of Biometrics

1. What is “biometrics”?

Biometrics is data that measures personal information about an individual’s physical or behavioural characteristics in order to verify their unique identity. It covers a wide range of personal characteristics including fingerprint identification, iris and retina scanning, face recognition, vein geometry and voice recognition.

Our school is intending to use fingerprint biometrics to assist with rapid student identity verification with guaranteed accuracy.

2. How will biometrics be collected?

Fingerprint sensors will be used to take an image of the finger which is converted to a mathematical algorithm of the fingerprint. This is an encrypted digital interpretation of the fingerprint image that is only usable on the devices that we use.

No fingerprint images will be stored, only the encrypted digital interpretation of the fingerprint image is stored on the device and on the device.

3. Who has access to the biometric data and the information associated with it?

The fingerprint scan is stored in the REACH Boarding System database in a proprietary format (an actual copy of the fingerprint image itself is NOT stored). Only the REACH BioPad fingerprint readers can recognize this format. Fingerprints are not transferred or shared with to any other systems.

4. Can my biometric image be used anywhere other than the School?

No. A fingerprint registered on one system will not be valid for another unique system. Only information stored on the database linked to the biometric scanner used is available when a fingerprint is scanned.

5. Can someone steal my biometric (fingerprint)?

A fingerprint is unique. No two people have identical fingerprints. It would be next to impossible for someone to steal someone else’s biometric (fingerprint) and the fingerprint itself is not stored by REACH, only an encrypted digital interpretation of the fingerprint image.

The Australian Privacy Principles

The Australian Privacy Principles (APPs), which are contained in schedule 1 of the *Privacy Act 1988*, outline how most Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses (collectively called 'APP entities') must handle, use and manage personal information.

While the APPs are not prescriptive, each APP entity needs to consider how the principles apply to its own situation. The Principles cover:

APP 1: Open and transparent management of personal information

APP 1 requires an APP entity to implement privacy practices, procedures and systems:

- to ensure compliance with the remaining APPs and
- that enable them to deal with inquiries and complaints.

It also requires them to develop and make readily available a policy about its management of personal information.

APP 2: Anonymity and pseudonymity

APP 2 entitles individuals to the option of anonymity or using a pseudonym, when dealing with an APP entity, except where impracticable or another prescribed exception applies.

APP 3: Collection of solicited personal information

APP 3, in summary:

- permits an APP entity to collect personal information only where reasonably necessary for one or more of its legitimate functions or activities
- requires personal information to be collected directly from the individual to whom it relates, unless impracticable or another prescribed exception applies and
- requires the consent from an individual in order to collect that individual's sensitive information, or another prescribed exception applies.

APP 4: Dealing with unsolicited personal information

APP 4 requires an APP entity that receives unsolicited personal information to determine whether it would otherwise have had grounds on which to collect it (i.e. under APP 3) and:

- where it does have such grounds, to ensure compliance with the remaining APPs or
- where it does not have such grounds, to destroy or de-identify the personal information (provided it is lawful and reasonable to do so).

APP 5: Notification of the collection of personal information

APP 5 requires an APP entity to notify an individual (or ensure they are aware), at or before the time of collection, of prescribed matters. Such matters include but are not limited to whether the individual's personal information is collected from any third parties, the purpose(s) of collection, to whom personal information is disclosed and the processes through which an individual can seek access and/or correction to their personal information, or otherwise complain about the way in which it is handled.

Compliance with APP 5 usually requires 'collection statements' to be included on or with forms, or other materials, through which personal information is collected. Such statements should refer and include a link to the APP entity's privacy policy.

APP 6: Use or disclosure of personal information

APP 6 prohibits an APP entity from using or disclosing personal information for a purpose other than the purpose for which it was collected, unless the individual consents, the individual would reasonably expect their personal information to be used for the secondary purpose, or another prescribed exception applies.

Such prescribed exceptions generally arise where the disclosure is necessary to protect someone's health or safety or is otherwise in the public interest.

APP 7: Direct marketing

APP 7 generally prohibits personal information to be used for direct marketing purposes unless the individual reasonably expects it, or consents to it, and prescribed 'opt out' processes are in place through which the individual can elect not to receive direct marketing communications (and the individual has not elected as such).

APP 8: Cross-border disclosure of personal information

If an APP entity is to disclose personal information to an overseas recipient, APP 8 requires it to take reasonable steps to ensure the recipient does not breach the APPs. This usually requires the APP entity to impose contractual obligations on the recipient.

Relevantly, if the overseas recipient does breach the APPs, the Privacy Act imposes liability on the APP entity that made the overseas disclosure.

There are exceptions to this obligation, including but not limited to where:

- the APP entity reasonably believes the overseas recipient is bound by a law or scheme that protects personal information in a substantially similar way to that of the APPs or
- the individual consents to the disclosure in the knowledge that such consent will negate the APP entity's obligation to ensure the overseas recipient does not breach the APPs.

APP 9: Adoption, use or disclosure of government related identifiers

APP 9 prohibits an APP entity from adopting, using or disclosing a government-related identifier unless:

- required or authorised by law
- necessary to verify an individual's identity and/or
- another prescribed exception applies.

Government-related identifiers are identifiers that have been assigned by a government agency including an individual's licence number, Medicare number, passport number and tax file number.

APP 10: Quality of personal information

APP 10 requires an APP entity to take reasonable steps to ensure personal information it collects, uses, discloses and holds is accurate, up-to-date and complete. Additionally, personal information can only be used or disclosed to the extent to which it is relevant to the purpose of the use or disclosure.

APP 11: Security of personal information

APP 11 requires an APP entity to take reasonable steps to protect information from misuse, interference and loss and from unauthorised access, modification or disclosure.

An APP entity must also destroy or de-identify personal information it no longer requires (unless otherwise required to retain it by law).

APP 12: Access to personal information

APP 12 requires an APP entity to provide an individual, upon request, with access to their personal information unless a prescribed exception applies.

APP 13: Correction of personal information

APP 13 requires an APP entity to take reasonable steps to correct personal information it holds upon request from an individual for correction or where it is otherwise satisfied, having regard to the purpose for which it holds the personal information, that the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading.

If an APP entity refuses a request for correction, it needs to provide the individual with the reasons for the refusal and may be required to associate with the personal information a statement evidencing the individual's view that the information is incorrect.

Where correction does occur, the APP entity may need to notify third parties to which the personal information, in its incorrect form, was disclosed.