Facial Recognition is coming to St Bernard’s High School

We’re excited to announce that Facial Recognition will soon arrive at St Bernards High School to offer a fast and straightforward payment experience for school meals.

It's important to us that everyone in our school community, including parents, guardians, and students, is well-informed about this new development and has all the information needed before opting to use this new service.

This document contains detailed information about Facial Recognition, how it works, how we will use the software, and most importantly, the benefits for students.

Why is St Bernard’s High School introducing Facial Recognition

Facial Recognition offers a quick and secure way for students to purchase school meal items without needing cash and the risk of losing cards or forgetting passwords. With Facial Recognition, students simply select their meal, look at the camera and go, speeding up the lunchtime service with a contactless point-of-sale experience.

This technology will be used as an additional authentication method at the checkout counters, providing faster service for students. Our goal is to help students reclaim time to enjoy their meal breaks and nutritious meals and make it easier to attend lunch clubs.

How the technology works

With Facial Recognition technology, students simply choose their meal, look at the checkout camera, and proceed with a quick and secure point-of-sale experience.

Facial Recognition is a biometric recognition method that works in the same way as other recognition technology. Like a PIN, a unique identifier is attributed to each student and matched at the till for quick and secure access to their cashless account.

An image of the face is captured, and the software turns unique features of the face geometry, such as the distance between the eyes and the distance from the top of the forehead to the chin, to create a unique identifier for each student.

When students pay for their meal items at the point of sale, the camera matches their unique identifier to their cashless account to take payment.

How the transaction process works:

1. **Consent**
Students must opt-in to use Facial Recognition before an image is taken. If students do not consent to using the software, the till operator cannot activate the Facial Recognition process.

2. **Capture:** The biometric system captures an image of the students' face. This image is not retained, stored, or distributed to third parties, and Facial Recognition cameras are only located at the point of sale for school meal transactions.

2. **Collection:** The system reads distinctive features from the image and processes it through an algorithm. This process turns the image into a unique string of characters, which serves as the student's unique identifier. This unique identifier is stored on a secure, encrypted database within the school and is used to verify students' accounts at the checkout.

3. **Identification:** During checkout, the cashier initiates the system to verify their account and process the transaction. The cashier must activate this process; the system is not live for students. A picture of the student is captured and processed through the algorithm to confirm their unique identifier and access their account. The image is not kept on record; only their unique identifier is stored.

Security of Facial Recognition

Biometrics, in this case, provides a unique identifier for the person present at the checkout. The unique identifier is created by processing the biometric capture through a mathematical algorithm, generating a unique number. Only this number is stored; the captured image is not retained. This data is encrypted using AES 256 (similar to encryption used by your online banking) and cannot be reversed to produce an image of the biometric, ensuring the highest level of security and compliance.

FAQs

What are biometrics?
Biometrics authenticates people based on their unique characteristics and identifies possible matches to ensure accurate and secure identification. Facial Recognition is a type of biometrics that we use in various aspects of life, including:

- **Security:** unlocking phones, accessing secure buildings, and logging into accounts
- **Identification**: faster check-ins at airports and hospitals
- **Convenience:** logging into computers and making payments for school meals

What student data is stored and where?
Biometric recognition operates on a closed-loop system, which means student data is stored on our secure database.

Can any other agency or 3rd party use the facial images?

No, the information is never shared, and the face template representing the students' faces is meaningless to anyone else. The software turns your child's image into a mathematical algorithm, and the stored information cannot be used to recreate the face image.

What happens when my child leaves the school?

All biometric data can be deleted; the school is the data controller and can delete the data from its databases. You can opt-out anytime, meaning the school will delete the biometric data.

What if I object to my child using Facial Recognition? Can my child still purchase school meals?

Parents and students reserve the right to object to using Facial Recognition. Any student not wishing to opt-in will be issued an alternative identification method, e.g., finger print or PIN.

Is this technology 'live'?

No; catering staff must activate the process at the point of sale for students that have consented to use Facial Recognition. The system is not live; the cameras only capture students' images for the transaction process when the PoS staff activates the software.

St Bernard's High School already has fingerprint biometrics

The school continuously strives to improve students' authorisation and school transaction experience. Students with consent to use fingerprint biometrics can eliminate the need to remember passwords or carry physical identification cards and benefit from a simple and safe authentication process. **If you currently use fingerprint biometrics, we would need authorisation to continue with this as it is a new system.**

Fingerprint biometrics works in the same way as other recognition technology. Like a PIN, a unique identifier is attributed to each student and matched for a quick and secure authorisation process.

How it works

- **Consent:** Students must opt-in to use fingerprint recognition before a fingerprint scan is taken. The biometric fingerprint scanner captures the unique trait (e.g., it takes an impression of the fingerprint). This fingerprint impression is not retained, stored, or distributed to third parties.

- **Capture:** During checkout, students place their fingers on the fingerprint scanner. In seconds, the system reads distinctive fingerprint features and processes them through an algorithm, which turns the fingerprint into a unique string of characters, serving as the students' unique identifier. This unique identifier is stored on a secure, encrypted database within the school and is used to verify students' accounts at the checkout.

- **Authentication**: The student's unique identifier securely matches the live fingerprint to their cashless account, and the transaction can now occur.

Advantages of using fingerprint biometrics in schools

Fingerprint recognition is a straightforward way to recognise students without risking losing cards or forgetting passwords. To register identify of students at the dining hall point of sale, fingerprint biometrics offers a straightforward way to identify and authenticate students.

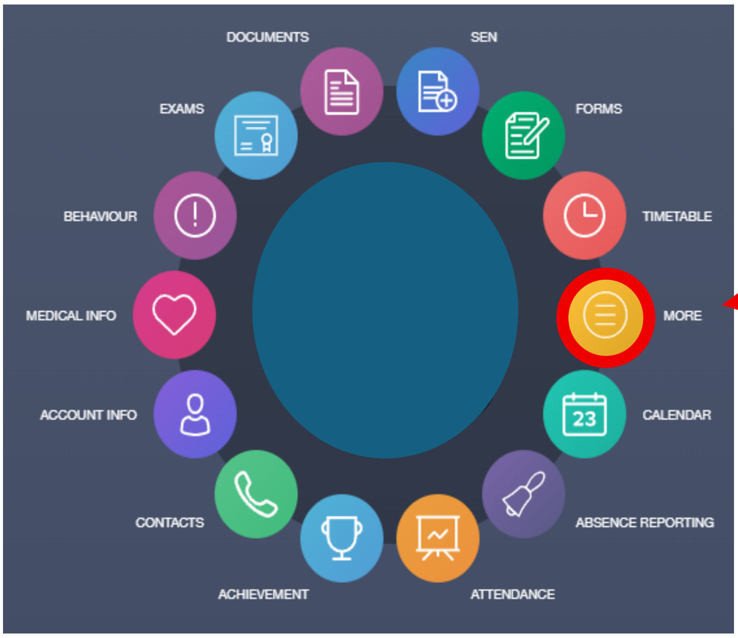
On average, it takes just seconds for a student to place their fingerprint on the biometric scanner and then the system to identify their account, offering a fast and efficient authentication process.

Security of fingerprint biometrics

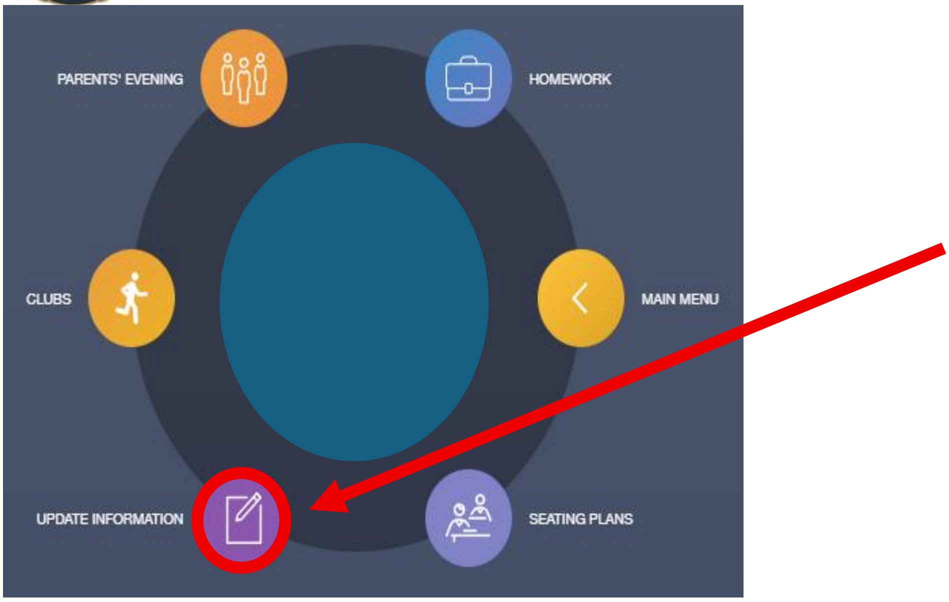
Biometrics, in this case, provides a unique identifier for the person present. The unique identifier is created by processing the biometric capture through a mathematical algorithm, generating a unique number. Only this number is stored; the captured fingerprint is not retained. This data is encrypted using AES 256 (similar to encryption used by your online banking) and cannot be reversed to produce an image of the biometric, ensuring the highest level of security and compliance.

How do I get started?

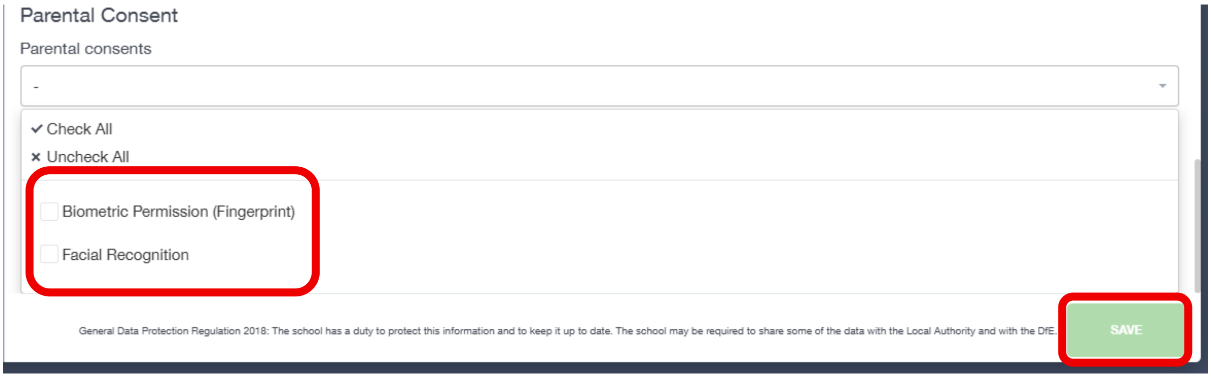
Login to Edulink - https://www.edulinkone.com/#!/login?code=stbernards



Click on the "MORE" button



Then click on the “Update Information” button



Parental Consent

Parental consents

-

✓ Check All

× Uncheck All

□ Biometric Permission (Fingerprint)

□ Facial Recognition

General Data Protection Regulation 2018: The school has a duty to protect this information and to keep it up to date. The school may be required to share some of the data with the Local Authority and with the DfE.

Then scroll down and click in “Parental Consent”

Then tick both boxes if you are happy to consent

Finally click on the “SAVE” button.