More information for schools

Useful information and frequently asked questions on Facial Recognition and Biometrics

Q. **What is Facial Recognition, and how does it work?**

A. Facial Recognition is a category of biometric technology that maps an individual's facial features (such as the length and width of the nose, the distance between the eyes and the shape of the cheekbones) mathematically and stores this data as a faceprint template. This faceprint is later used as a basis for comparing data captured from faces in an image to identify an individual.

Facial Recognition is now used for many applications, from security to payments. Currently, the most commonly utilised method of Facial Recognition is unlocking mobile phones, where users can unlock their device by simply looking at the camera.

Q. **Why is CRB Cunninghams using Facial Recognition?**

A. CRB Cunninghams have used biometric data (in the form of fingerprints) since 2008 to quickly and securely identify a user on the cashless system to pay for their school meals. CRB Cunninghams started exploring the possibility of using Facial Recognition as a new identification method in late 2019 but decided to expedite this development due to the Coronavirus pandemic.

Facial Recognition retains the speed and security benefits available with fingerprints but eliminates the requirement to physically touch a scanner, making purchasing school meals completely contactless.

Q. **How is the data stored?**

A. Facial Recognition data is a unique string of characters known as a faceprint template. This data is encrypted using AES 256 and is either stored on a school server within the secure school network or hosted on a secure Azure server by CRB Cunninghams.

Q. **Do you also store a photo alongside the faceprint template?**

A. Unlike fingerprint recognition (where we do not store an image of the fingerprint), we store a photo along with the faceprint template. The cashless system has always stored a user's photo, which is used as an added verification by the canteen staff.

Q. **How secure is Facial Recognition?**

A. CRB Cunninghams only employ this technology at the point of sale as this is attended to and operated by an authorised staff member.

Q. **We already have permission to store a person's photo; do parents/users need to grant explicit consent before using Facial Recognition?**

A. Yes. Before a user is allowed to use Facial Recognition software, they must give explicit permission to do so.

This permission status is recorded and set within the system, and only users with their permission updated to 'Allowed' can use Facial Recognition. If this status is set to 'Pending' or 'Denied', the system will not authorise Facial Recognition.

Q. **A parent/user has previously granted permission to use fingerprints; do they also need to give explicit consent before using Facial Recognition?**

A. The school (as the Data Controller) decides this. If the parent/user has previously granted explicit consent using fingerprints, they have consented to the using special category data Biometrics under GDPR, as the type of biometric data is not explicitly mentioned.

CRB Cunninghams would advise that gaining updated permission where the user/parent has explicitly consented to the using Facial Recognition would be the best practice. However, at a minimum, the school should be wholly transparent and publicise that Facial Recognition is being introduced and allow parents/users to update their consent in line with this additional information.

The system would still need to be updated to set the facial recognition permission status against each user that has granted permission before it would allow for capturing an individual's faceprint template.

Q. **If a parent/user does not wish to grant permission to use Facial Recognition, how would they access the system?**

A. Facial Recognition is an additional authentication method for our cashless catering systems. If a parent/user does not wish to grant consent, the school can provide an alternative ID method, such as fingerprints, card, PIN, or manual operator lookup.

Q. **A parent/user previously granted permission but now wishes to withdraw. How easy is this to do, and what happens to the data?**

A. Should a parent/user withdraw consent, their permission status within the system can easily be updated to 'Denied'. When the permission status is updated to no longer be 'Approved', any faceprint template data will be automatically removed as part of this process.