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 then later used as a basis for comparison with data captured from faces in an image to identify an individual.

Facial recognition is now used for a multitude of 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 are 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 this development was expedited due to the Coronavirus pandemic.

Facial Recognition retains the speed and security benefits that are available with fingerprints but eliminates the requirement to physically touch a scanner making the purchasing of 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 with fingerprint recognition (where we do not store an image of the fingerprint), yes, we do store a photo along with the faceprint template. The cashless system has always stored a user’s photo as this is used as an added verification by the canteen staff.

**Q.** **How secure is the use of facial recognition?**
**A.** CRB Cunninghams only employ the use of this technology at the Point of Sale as this is attended and operated by an authorised member of staff.

**Q.** **We already have permission to store a person’s photo, do parents/users need to grant explicit permission 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 that have had their permission updated to ‘Allowed’ would be able to use Facial Recognition. If this status is set to ‘Pending’, or ‘Denied’, the system will not allow the use of Facial Recognition.

**Q.** **A parent/user has previously granted permission for the use of fingerprints, do they also need to grant explicit permission before using facial recognition?**
**A.**This is for the school (as the Data Controller) to decide. If the parent/user has previously granted explicit consent for the use of fingerprints, then they have consented to the use of 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 use of facial recognition would be the best practice. However, at a minimum, the school should be wholly transparent and publicise that the use of facial recognition is being introduced and allow parents/users the opportunity 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 the capturing of an individual’s faceprint template.

**Q.** **A parent/user does not wish to grant permission for the use of 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, they can be provided with an alternative method of identification, 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.