OUR BIOMETRIC DATA SYSTEM – ADDITIONAL INFORMATION

We have asked you for consent to process your child's biometric data (fingerprint) for the purposes of the cashless payment system in the school. Biometric data is categorised as special category data so it requires additional protection when it is processed by an organisation. Please therefore find below additional information about the system. This gives you an explanation of how the biometric data system is set up, how we ensure the data is held securely, how it is collected, who precisely has access to it and for how long it is kept. At the end you will find some FAQs.

How the biometric system works

Process for using a biometric system

- On signing up to the system your child's fingerprint is mapped based on certain points which are called minutiae points. These are the points where a fingerprint ridge ends or splits in two.
- Typically, between forty and sixty points are mapped depending on the characteristics of the finger. This generates a unique numeric identifier (a string of characters) called a template.
- Typically, the template comprises roughly 34 characters. (This is an example code - DF77B4A9-D819-4A66-B803-BFABEB9D3B37) It is only this number that is stored in the system.
    - The template cannot be reverse engineered to create a usable fingerprint. This is because the level of detail stored in these data points is well below the level of detail needed for forensic identification of a person.
    - The set of numbers will be unique within populations of hundreds, or a few thousands, of people. However, in a wider population, the system is not accurate enough for the templates to be usable for forensic matching with any degree of certainty. A court of law would not be able to use this information as evidence, for example.
    - In addition, the unique numeric identifier is encrypted using AES256 which is a commonly understood encryption standard that is also the same level of security used by banks and other financial institutions to protect sensitive customer information. So even if an outside actor could get into the system, they
    - would need to break the encryption to gain access to the unique numeric identifiers. And, as stated above, if they managed this these identifiers cannot be reverse engineered to create a usable fingerprint.
- When purchasing something at the till the student places their finger on a scanner and the software reads the same key features (unique patterns of a fingerprint) and compares this against the database of templates of registered users.
- When the system finds a match (template), it links to a pre-existing database ID number which in turn links to the payment system so that payment can be authorised. Balance top-ups are updated from the online payment system to the catering system in near real-time, while balance settlements are synchronised from the catering system back to the payment system at the end of the day. The system also synchronises with the school's management information system (MIS) at the end or beginning of each day, depending on the system, to ensure records are up to date (Free School Meals, processing new users and leavers).
- The combination of encrypted templates, AES256-protected local servers, VLAN isolation, firewall restrictions, and live-finger detection technology ensures a highly secure and reliable catering system (although it should be borne in mind that no data-processing system is 100% risk free). Communications between applications, the online payment system, and the database are also encrypted using AES256.

FAQs

Is the fingerprint stored?
No. The finger print is not stored.

Where is the biometric data stored?

The data is held on the school servers.

How secure is the stored data? What would happen if somebody stole it?
The system database is protected by a licence key. This means that the database and any backup of its contents can only be accessed on licensed hardware. The hardware is stored in the school's own secure facility, so that the encrypted data is only available to the registered licensee. Even if the school's security were to be compromised and a backup of the database stolen, the encrypted data would still be unreadable given that it is encrypted with AES 256.

What about network security?
Firewall rules restrict communication to only the catering tills and defined admin user devices on the school network. Both the server and tills reside on private, protected VLANs (Virtual Local Area Networks) that are not accessible from other internal VLANs used for general school network traffic. Only the school (and not the provider of the system) has access to the data.

Could the police or a court of law use the fingerprints stored in the system's database?
The fingerprint is not stored. The recorded templates consist of a set of numbers, which represent each person. This set of numbers will be unique within populations of hundreds, or a few thousands, of people. However, in a wider population, the system is not accurate enough for the templates to be usable for forensic matching with any degree of certainty. A court of law would not be able to use this information as evidence.

What if a parent/carer or the student didn't want the student's fingerprint to be used?
At the school there is always an alternative means of payment available which is by the school issuing the student with a pin code, or manually accessing the students account by their name. A student or parent/carer has the right to withdraw consent completely for the student's biometric data to be used in which case they will be provided with an alternative means of payment and their biometric data will be deleted from the system.

Deletion of data
An individual's template is deleted once they leave the school or consent to use the data is withdrawn either by a parent/carer or the individual themselves.