Protection of Biometric Data Policy

Policy approval date	29.06.2021
Policy review date	June 2023
Policy Lead	Data Protection Officer
Trustee approval	Trustee Approval
Committee responsible for policy	Trust Standards Committee

Protection of Biometric Data Policy

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The Trust will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the Trust's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can object to participation in the Trust's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the Trust's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the Trust will delete any relevant data already captured.

The Use of Biometric Recognition System

The Trust currently uses BioStore as the central database, which stores the information which identifies pupils uniquely to each of the applications used at the schools. BioStore requires each pupil to register only once, usually placing a finger on a fingerprint scanner, although other identification methods are available, such as a PIN number.

BioStore does not store images of fingerprints on its system, and never will. Only mathematical representations of certain points of a finger print are recorded, typically between 10 and 60 depending on the characteristics of the fingerprint. This data is encrypted so it is impossible to recreate the original fingerprint.

The BioStore database is protected by a license key, meaning 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 a 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.

Appendix A – copy of letter to parents

Appendix B – BioStore security Document

Appendix A

Dear Parents/Carers

Cashless Catering System

Clarion Academy Trust operates a cashless catering system. This means that all transactions for food and drinks during morning break and lunchtimes are made by either using a PIN number or biometric identification, namely a code generated from a digital fingerprint.

We have found the advantages of this system to be:

- Reduction in queuing time
- Reduction in opportunities for theft or loss of money
- Students entitled to free school meals will use the same system and are therefore unidentifiable
- Funds can be credited via Wisepay from home and are available immediately
- Parents are able to view transactions and purchases via Wisepay

Our preferred method of completing a transaction is by Biometrics, that is, the use of a fingerprint. This is a system that has been used successfully since 2017.

We would like to make it clear that Clarion Academy Trust complies at all times with Data Protection Act and with the guidance given by Becta and by the Information Commissioner's Office regarding the use of biometric data.

Fingerprint images are not be stored by the system (instead, a set of coordinates is translated into a string of numbers and encrypted). The encryption method used by the system is a high level, industry standard method. The data held could not be used to recreate a fingerprint image, nor could it be used in a forensic investigation. Further information regarding Biometric security can be found on our website.

Once registered, cash can be credited to their account via a cash loader in school at this point. The cash loader will remain in school, but we strongly recommend you credit funds via Wisepay.

We will also offer an opportunity to opt out for those students who, upon consideration, feel that they would rather not have their biometric data recorded. A PIN will be issued as an alternative.

If you would like more information or the chance to discuss this further, please feel free to contact me.

Yours faithfully

Appendix B

BioStore Security

There has been a fair amount of controversial press around the issue of biometrics. BioStore strongly recommends that schools consult with and address issues raised by pupils and their families, before implementing any kind of biometric system.

BioStore Partners will always offer an opt-out option for individuals who are uncomfortable with using biometrics. Our system can be used with any combination of finger recognition, cards, PIN codes, usernames and passwords, and more. Each BioStore Partner will offer particular opt-out options for use with their applications.

Encryption

The BioStore database is encrypted using AES256 – an industry standard and highly secure technology. All communications between applications and the database are also encrypted using AES256. Each school has its own secret unique group of AES256 encryption keys, which means that the database and any backup of its contents can only be accessed on licensed hardware, and the encrypted data is only available to the registered licensee. Even if a school's security were to be compromised and a backup of the database stolen, the encrypted data would still be unreadable, even by another school.

AES256 is the same encryption technology that is used in Microsoft's BitLocker disk drive encryption, and is certified by the National Security Agency of America to be used to protect Top Secret information.

It has been calculated that it would take all the computers in the world 3x10^51 years to decrypt a file that has been encrypted with AES256 using a brute force method.

Finger Recognition

When a person registers their finger in BioStore, no image is saved. Instead approximately 40 to 60 minutia points are recorded – minutia points are the location and direction of where a ridge ends or splits in two. The rest of the information from the finger scan is discarded.

The information used is encrypted and called a template. The data is extremely secure in its encrypted form, but even if it were not encrypted it is impossible to recreate the original image of the finger from this data. The BioStore system only stores a short string of encrypted numbers – too few to provide enough detail for the original print to be reconstructed.

Deleting data from BioStore

User records can either be made inactive or removed from the BioStore database. Making people inactive is a temporary measure which makes no change to their data but disables the user's access to connected services until they are made active again. Removing records from the BioStore database will delete and completely overwrite all of the user's information, including any finger scans or other identification methods that were associated with the user's record.

Common Objections

One of the objections raised to the use of biometrics in schools is concern about the security of BioStore data while it is in use by a school. The following points attempt to address this issue:

- The BioStore database is stored on the school's servers, not outside of the school network.
- We would expect a school to apply the same level of physical security to biometric data as they do to other sensitive data held within a school.
- We would expect a school to destroy the records of pupils who have left the school.
- There are two steps in deleting records from BioStore – Records are first made inactive (so they remain in the database but have no functionality), and then they can be removed from the database. This process completely deletes and overwrites all information in the record, including any enrolment data.
- BioStore uses AES256 encryption – a US Government and worldwide encryption standard. This also applies to communication between different parts of the BioStore system.

- Each school has a unique key that is used for encrypting the database, so a database cannot be transferred to another school's system and viewed.

Another objection is caused by concern as to whether an identity thief, having stolen a BioStore database, may be able to reconstruct fingerprint images and use them to commit identity fraud.

- Because only certain points of a fingerprint are recorded, it would only ever be possible to recreate a partial fingerprint image.

- In order to recreate a partial fingerprint image, you would have to be able to decrypt the template data, have access to the template algorithm to be able to interpret the numerical string that is generated, and have a method of generating an image from the data.
- The important point in this scenario is that having an image of a fingerprint (partial or otherwise) is not much use anyway. The fingerprint scanners supplied by BioStore use 'live finger detection' technology, which can detect fake fingerprints. This technology will continue to develop and become even more sophisticated.

- It is worth noting that other institutions that use fingerprint technology are unlikely to rely on a single method of identification. This would certainly apply if banks were to adopt fingerprint technology. They would use (as they do now) multi-factor authentication and probably a mixture of biometrics (such as facial recognition, finger vein or iris scans), and 'changeable' data such as PIN and security codes, passwords and signatures. Should there be any suspicion that the integrity of a person's fingerprint as a secure means of authentication has been compromised, it would be possible to use other methods of identification or even just different fingers.

If, in the future, there were significant concerns that fingerprint data had been or could be reverse engineered in such a way that it were possible to trick a fingerprint scanner, fingerprint recognition would be invalidated as a secure form of identification and would not be used in secure environments, such as banks.
Even if this was possible, reverse engineering template data is a very labour intensive way of getting a partial fingerprint image. It is possible to lift someone's fingerprints from items they have touched.
The issue is not that of being able to obtain a fingerprint image, but that it is not a lot of use once you have it.

Another common objection is that fingerprint templates could be used in forensic investigation.

- At best, partial fingerprint images could be used to inform a police line of enquiry. Fingerprint images obtained from BioStore have never and will never be used as admissible evidence in a court of law.

- When considering issues relating to banking and forensic investigation, it is worth noting that the false acceptance rate is approximately 0.00001%, or 1 in 100,000. This is low enough to give a very accurate and secure system within an organisation such as a school, but is not accurate enough to be able to pinpoint somebody within the wider population.

Other Identification Methods

It is worth considering other forms of identification, just for comparison.

Take a signature, for example. Although it is possible to change a signature, people rarely do. Signatures are on record at the passport office, the DVLA, banks etc. They are written or printed on driving licences, passports, letters, cheques and bank cards and could be copied should these items fall into the wrong hands. The reason that this is not a complete security disaster is similar; a photocopy of a signature is not an accepted secure identification method. A pen-and-ink signature is required in any secure context, and because multi-factor authentication in some shape or form is usually in operation, other proof of identity is also required alongside the signature.

Your face is a biometric form of identification and it is not changeable. Your face is recorded in a large number of places – Management Information Systems, passports, driving licences, CCTV footage, social networking sites, etc. In some cases you have given your permission, and in other cases you have not. Facial recognition may be used as a method of authentication in the future, so it is worth considering why we don't (generally speaking) have the same reservations about images of our faces being recorded and stored in the same way that we do with our fingerprints.