

Biometrics at Charters School

Frequently Asked Questions

What is Biometric authentication?

Biometric identification is one way of quickly and uniquely recognising users in a way that cannot be forgotten or lost. It only needs the user to register once for all systems in the school for which parental permission has been given.

How does it work?

By taking an image of an individual's biometric we can turn this information into a digital signature that can be recognised by our systems. When the student places their biometric input (fingerprint) on the scanner, the software matches their biometric image with the unique digital signature held in the database. Students will then be able to purchase food and check account balances by simply placing a finger on a digital scanner.

What does the law say?

The Information Commissioner considers all biometric information to be personal data as defined by the Data Protection Act 1998; this means that it must be obtained, used and stored in accordance with that Act. The Protection of Freedoms Act 2012 changed the way that schools are allowed to use biometric data in schools when used as part of an automated biometric recognition system. There are links at the end of this document to Government Guidance on biometrics in schools.

What provisions are made to protect data in line with GDPR NIS directives?

The Information Commissioner's Office (ICO) is currently consulting on guidance for this, as soon as this is available we will update our policies and procedures to ensure compliance.

Can biometric information in use at Charters School be used by any other agency?

No, the software we use turns the biometric image into a mathematical algorithm. The image of the biometric is then discarded. The information that is stored cannot be used to recreate an image of the child's biometric.

What happens when a student leaves the school?

When a student leaves school all data relating to their biometric will be permanently deleted within three months of a student leaving.

What happens to the fingerprint?

When a student registers to the biometric system, their finger is placed on to a fingerprint scanner. The fingerprint is then converted into a collection of data points via a mathematical algorithm. This data is then encrypted and stored on the pupil's account to be used as their unique identifier.

Are the fingerprints stored?

No. The fingerprint is only used to generate a collection of data points which is then encrypted. The fingerprint reader looks for specific patterns and unique identifiers on the finger, assigning specific data to each point. The fingerprint is never actually recorded.

Can the secure data be reversed to produce a fingerprint?

No. The data points produced by the algorithm can't be reversed to produce a full fingerprint. The data is fully encrypted to military grade standards and even if this was to be broken, trying to reproduce a fingerprint from the data points could never produce anything usable.

Is my student's data secure?

The BioStore database is protected by a licence 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 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.

Data will be backed up daily by Charters School in line with normal procedures. The biometric data itself is encrypted with a 32bit fully encrypted algorithm. The network is protected from outside attacks using a threat management system which includes a firewall.

Can the police use the biometric data as a fingerprint?

Biostore at Charters only store encrypted data points from a finger scan. Even if we were asked to decrypt and reverse the algorithm for the police, the image produced would not be accurate enough for forensic matching and would not be admissible in court. The police would not be able to use the data points for their databases as the algorithms don't match.

I have identical twins; won't they have the same fingerprint?

Identical twins share many physical similarities but have different fingerprints and therefore digital signatures.

What about cuts or other injuries?

Unless the injury results in a severe disfigurement to the finger, the biometric system will still be able to recognise the user.

What if my child has a medical condition that makes the fingerprint difficult to read?

Biostore cards can be made available to any student who cannot use the scanner.

What about hygiene when everyone is touching the same area with their fingers and then eating?

Antibacterial gel will be made available at the entrances to the dining hall. The scanners will be part of a daily cleaning rota and will be regularly sanitised.

What if the system breaks down?

The school has clear Service Level Agreements in place with Biostore which means a quick turnaround for failed hardware and online support for software issues. If for any reason the biometric scanner does not recognise a fingerprint, there will be an option to look up an individual via surname and photo ID.

I don't want my child to be entered in to the biometric database, what alternatives are there?

Any student who wishes to opt out will be issued with a Biostore card. This will initially be free of charge but if lost, there will be a replacement cost.

I'm happy for my child to be on the biometric database but what if he/she doesn't want this to happen?

The Protection of Freedoms Act 2012 has legislated that if a pupil under 18 objects or refuses to participate (or to continue to participate) in activities that involve the processing of their biometric data, the school must ensure that the pupil's biometric data are not taken/used as part of a biometric recognition system. A pupil's objection or refusal overrides any parental consent to the processing.

Further information and guidance can be found via the following links:

Department for Education's *Protection of Biometric Information of Children in Schools – Advice for proprietors, governing bodies, head teachers, principals and school staff*:
<http://www.education.gov.uk/schools/adminandfinance/schooladmin>

ICO guide to data protection for organisations:

http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx

ICO guidance on data protection for education establishments:

http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx