

Protection of Biometric Information Policy

SLT	Rob O'Halloran
Committee	Staffing & Resources
Date Agreed	Spring 2026
Review Date	Spring 2027

The use of Biometrics within Deptford Green School

Students and Staff access our cashless catering system via fingerprint recognition which will identify them. Staff also access printing and photocopying. The software used to capture the appropriate information is BioStore. BioStore is a central database located within a school, which stores the information which identifies students and staff uniquely to each of the applications used at the school.

BioStore requires everyone to register only once, usually by placing a finger on a fingerprint scanner, although other identification methods are available. BioStore's centralised system speeds up the registration process – each student need only register once, no matter how many applications requiring identification are in place at the school. With a Biometric system, students cannot borrow or steal credentials from each other, reducing the opportunities for bullying. Queues are reduced because the rate of identification of students is quickened. Students need no longer carry cards, remember PIN numbers, or use cash to buy a meal. Biometric systems save time and money for both school and students because the need to replace lost cards and forgotten passwords is eliminated.

BioStore does not store images of fingerprints on its system, and never will. Only mathematical representations of certain points of a finger image are recorded, typically between ten and sixty depending on the characteristics of the finger. This mathematical data is encrypted and is called a template. The data is extremely secure in its encrypted form, and even if it were not encrypted it would be impossible to recreate the original fingerprint image from the stored data.

It is not possible to recreate a fingerprint from the data stored by BioStore as the only stores a short string of encrypted numbers, too little data for the original print to be reconstructed.

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.

The fingerprint template stored in the database is merely a string of encrypted numbers. If this string of numbers were to be removed from the database, it would be useless, because it cannot be recognised as a fingerprint. A fingerprint scanner checks for a real finger – it does not recognise a string of numbers.

BioStore does not store fingerprint images. The recorded templates are comprised 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.

Even identical twins have different fingerprints and will not be mistaken for each other by BioStore. In very rare cases there are people born without fingerprints. Occasionally someone's fingerprints may deteriorate because of exposure to some chemical products, and sometimes temperature changes can cause reduction in fingerprint quality. However, a cut finger would not cause any problem for BioStore, unless it resulted in major disfigurement.

Alternative identification methods - PIN numbers - are always available in BioStore systems. Students unable to provide biometric data can opt to use this method, as can any student who prefers not to use biometrics. The school will issue any student who wishes to opt out of the biometric system with an PIN numbers and photo lookup.

Appendix 1: Letter of Consent to Use Student Biometric Data

(please note that a form of this is held on the admissions form)

Dear [parent/carer name],

At Deptford Green School, we use Biostore fingerprint scanning technology to access the school meals system. This information is held securely in school and helps us operate more efficiently. We need your consent to use your child's data in these systems. Please check the boxes below and send the form back to the school office if you're happy for these activities to go ahead.

If you're not happy for us to use information in this way, that's no problem – we will accommodate your preferences. You can object at any time to your child's participation in these systems, and you can also withdraw any consent you give us whenever you want. If you ever want to withdraw consent, or object, please let us know by emailing info@deptfordgreen.co.uk or sending/handing in a letter to the school office.

Our privacy notice has full details on how we use your child's personal information, including fingerprints. <https://www.deptfordgreen.lewisham.sch.uk/about-us/privacy-policy/> You can also request a copy of the Protection of Biometric Information Policy

If you have any other questions, please get in touch.

Yours sincerely,

Consent Form: Please tick one

Biometric Data	Tick
I am happy for the school to use my child's fingerprints for them to receive school meals.	
I am NOT happy for the school to use my child's fingerprints in these ways.	

Name: _____

Signature: _____

Date:_____