

All Saints Schools Trust



Biometric Data Usage Policy

	Date
Agreed by Trust Board:	March 2020
Lead:	HR Committee
Review date:	February 2024

Biometric Data Usage Policy

Introduction

Context Biometric Data processes are increasingly being used in schools for operational purposes such as catering, library and registration. Clearly such processes offer many potential efficiency benefits. Nevertheless All Saints Schools Trust recognises and understands that use of such Biometric Data processes is contentious. Consequently we will abide by:

- all relevant and current legislation (eg Protection of Freedoms Act 2012)
- any statutory guidance or codes of practice issued by DfE, the Home Office and/or the Information Commissioner.
- Furthermore, we also believe that proper explanation of the reasons why we would like to establish biometric data systems, how those systems operate and the advantages that they will bring students and school alike should help to alleviate any concerns.

Principles

This policy relates to biometric data that can be used for the purpose of electronically identifying and authenticating an individual. It does not apply to ordinary photographs or videos including digital photographs unless they are used for electronically verifying an individual's identity.

Typically the biometric data covered by this policy will include fingerprint and iris scans.

Practices and procedures

At present All Saints Schools Trust does not use or store biometric data apart from Occold Primary which uses finger print scanning as an entry mechanism. If any any point we universally introduce this we would abide by the following:

1. Biometric data will be held in compliance with Data Protection legislation on All Saints Schools Trust secure computer systems and will not be linked to any other computer systems or databases outside the direct control of Trust schools.
2. Biometric data will be used only for the purposes specified in advance and for which the individual has given written consent (and that consent has not been withdrawn in writing by the parent/guardian of a student under 18). For example, where biometric data has been collected to facilitate the borrowing of books from schools it would not also be used to assist the identification of a finger print found on stolen property.
3. Biometric data will be encrypted to guarantee confidentiality and to guarantee that the original image cannot be reconstructed. (Typically a fingerprint scan will be sampled at a number of points and a numerical code generated and stored in a computer record for the individual. The fingerprint image will not be stored. Each time a fingerprint is scanned to authenticate a transaction a numerical code is generated and compared to the original stored code.)
4. Biometric data will not to be disclosed to any third party (except in so far as is necessary for them to operate or maintain the system on behalf of Sandbach School) unless the student (and their parent or guardian in the case of minors) consent in writing or where required by law.
5. At least 2 calendar weeks before introducing a new biometric data scheme All Saints Schools Trust will distribute a briefing document to the parent/guardian of all students that will be affected by the scheme explaining why we would like to introduce the scheme and the advantages that it offers. The briefing document will contain a form to be completed and returned to the school for the parent/ carer to provide written consent to their child(ren), if under the age of 18, participation in the scheme. → The briefing document will also be published on the school web site and be made available to all pupils, staff, volunteers and governors.
6. In addition to written parental consent for students' participation, the school will only enrol on the system those individual users (students and others) who consent to the collection and storage of their biometric data.
7. A student or any other user will have a clear and unambiguous right to withdraw their consent to participation in the biometric data system at any time.
8. Biometric data held will be destroyed when the student leaves the school or by written request of the student, or if the student is under 18 by their parent/guardian at any time. Consent/exemption forms will be destroyed 6 years after the student leaves school.