

# THORPE HALL SCHOOL

## Biometrics Policy

### **What is Biometric Data?**

Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns and hand measurements. At Thorpe Hall School, we use fingerprint mapping for our cashless catering system.

All biometric data is considered to be special category data under the UK General Data Protection Regulation (UK GDPR). This means the data is more sensitive and requires additional protection as this type of data could create more significant risks to a person's fundamental rights and freedoms.

This policy complies with The Protection of Freedoms Act 2012 (sections 26 to 28), the Data Protection Act 2018 and the UK GDPR.

The School has carried out a Data Protection Impact Assessment with a view to evaluating whether the use of biometric data is a necessary and proportionate means of achieving the legitimate objectives set out below. The result of the Data Protection Impact Assessment has informed the School's use of biometrics and the contents of this policy.

### **The Legal Requirements under UK GDPR**

'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it.

As biometric data is special category data, in order to lawfully process this data, the School must have a legal basis for processing personal data and a separate condition for processing special category data. When processing biometric data, the School rely on explicit consent (which satisfies the fair processing conditions for personal data and special category data). Consent is obtained using the providers consent form OR via the School's digital consent form.

The School processes biometric data as an aim to make significant improvements to our canteen and lunch facilities. This is to ensure efficiency, to do away with the need for swipe cards and cash being used.

### **Consent and Withdrawal of Consent**

The School will not process biometric information without the relevant consent.

#### *Consent for pupils*

When obtaining consent for pupils, both parents will be notified that the School intend to use and process their child's biometric information. The School only require written consent from one parent (in accordance with the Protection of Freedoms Act 2012), provided no parent objects to the processing.

If a parent objects to the processing, then the School will not be permitted to use that child's biometric data and alternatives will be provided.

The child may also object to the processing of their biometric data. If a child objects, the School will not process or continue to process their biometric data, irrespective of whether consent has been provided by the parent(s).

Where there is an objection, the School will provide reasonable alternatives which will allow the child to access the same facilities that they would have had access to had their biometrics been used.

Pupils and parents can also object at a later stage to the use of their child's/their biometric data. Should a parent wish to withdraw their consent, they can do so by writing to the School at [sec@thorpehallschool.co.uk](mailto:sec@thorpehallschool.co.uk) requesting that the School no longer use their child's biometric data.

Pupils who wish for the School to stop using their biometric data do not have to put this in writing but should let their form tutor know.

The consent will last for the time period that your child attends the School (unless it is withdrawn).

### **Retention of Biometric Data**

Biometric data will be stored by the School for as long as consent is provided (and not withdrawn).

Once a pupil leaves, the biometric data will be deleted from the School's system no later than 72 hours.

### **Storage of Biometric Data**

At the point that consent is withdrawn, the School will take steps to delete their biometric data from the system and no later than 72 hours.

Biometric data will be kept securely and systems will be put in place to prevent any unauthorised or unlawful access/use.

The biometric data is only used for the purposes for which it was obtained and such data will not be unlawfully disclosed to third parties.

Policy created:	Feb 25
Policy approved:	Mar 25
Next review date:	Feb 27