Processing of Biometric (Fingerprint) Data for Cashless Canteen Payments

Submitting controller details

Name of controller	St Marks Catholic School
Title of DPO and Name of DPO	External DPO – Richard Maskrey Internal DPO - Emma Gritten – CFO

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
The processing involves pupil and staff biometric data (in the form of a fingerprint) which is used as identification for pupils and staff to allow access to their catering accounts on the Sharps till system. The system allows identification at the point of service delivery via EPOS terminals and coin & note revaluation units. As the data is biometric, which is deemed to be a special category of data under the Data Protection Act 2018, the school has deemed it necessary to complete a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
The source of the data is the pupil or staff member (finger print). Consent is provided by the pupil's parent/carer to allow the biometric data to be taken. This is done when the pupil transitions to the school. The processing includes: • Recording pupils/staff biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner. • Storing pupils/staff biometric information on a database.

- Using pupils/staff biometric data as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise pupils.

The biometric data is held on the Sharps till system. The biometric data (fingerprints) are stored as a series of data points, converted from images by a mathematical algorithm. These data points cannot be used to reconstruct a useable fingerprint even with the algorithm available. The level of detail stored in these data points is well below the level of detail needed for forensic identification of someone and would be completely inadmissible, both in terms of quality and legality, in court. The data points are encrypted before being stored.

Sharps act as a data processor when they remotely connect to the school to assist with maintenance routines and imports.

The school's caterers Cucina can access the Sharps till system but do not have access to the biometric data itself.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The nature of the data is fingerprints which are stored as a series of data points, converted from images by a mathematical algorithm. These data points cannot be used to reconstruct a useable fingerprint even with the algorithm available. The level of detail stored in these data points is well below the level of detail needed for forensic identification of someone and would be completely inadmissible, both in terms of quality and legality, in court. The data points are encrypted before being stored. The data does not include criminal offence data.

A finger print is taken for every pupil whose parent/carer has provided consent. . A finger print is also taken for all staff who have provided consent.

The data is held until the pupil withdraws their consent or leaves the school in line with the Department for Education's school data retention schedule and is archived data on an annual basis.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Consent has been provided by all parents/carers to allow the school to process the data. The data belongs to children (between the ages of 11 to 18). Consent is provided under Section 26 of the Protection of Freedoms Act 2012. Written consent is sought from at least one parent of the pupil before the School collects or uses a pupil's biometric data.

Consent has been provided by all staff to allow the school to process the data. Consent is provided under Section 26 of the Protection of Freedoms Act 2012.

Parents/carers, pupils and staff can object to the processing of biometric and can withdraw their consent at any time.

The school has no concerns over the processing. This type of data is held by a significant number of schools and is not considered to be novel or contentious.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

The purpose of the processing is to allow pupils quick and easy access to their catering accounts without needing to remember a pin number or use an electronic card (which is often lost or misplaced). It therefore allows a secure method of identifying pupils and is also quick, which is critical to ensure that large queues do not build up during the busy lunchtimes and breaktimes.

The processing allows the school to administer the Free School Meal system more efficiently, including the facility to monitor which vulnerable children have taken a meal.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

The school does not consider that any further consultation is necessary. The system has been in place for a number of years. There have been no complaints or concerns parents/carers, pupils and staff regarding the processing of this data.

Any pupil whose parent/carer does not provide consent for the system will instead be issued with a card which allows access to their catering account. The school therefore considers that it has reasonable alternative arrangements in place for those that do not have consent.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The biometric system operates on the basis of consent. The school has considered that using biometric data for identification purposes is the most practical way of identifying pupils for this purpose. The data is not used for any other purpose.

Parents and carers, pupils and staff are given full information about the biometric system. This DPIA should be read alongside the Protection of Biometric Information Policy which is available from the school's website. The school has a Data Protection and Breach Notification Policy which should also be read alongside this DPIA.

If the data is used for any other systems, consent will be obtained from the parent/carer or member of staff to remove the risk of function creep.

The data is not transferred outside of the UK.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Data is not held securely	Remote	Minimal	Low

Data could be used to identify the individual	Remote	Minimal	Low
Biometric data is not deleted when the pupil/staff member leaves school	Possible	Minimal	Medium
Biometric data is recorded without consent	Remote	Minimal	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
Data is not held securely	The level of detail stored in these data points is well below the level of detail needed for forensic identification of someone and would be completely inadmissible, both in terms of quality and legality, in court. The data points are encrypted before being stored. The encryption standard used for encrypting the data points is AES 256.	Reduce risk	Low	Yes
Data could be used to identify the individual	Consent forms are completed and the information is held on SIMs. These are checked before the biometric data is taken to ensure that only pupils for whom a consent form is held have their data taken.	Reduce risk	Low	Yes
Biometric data is not deleted when the pupil/staff member leaves school	Procedures in place to process leavers on a timely basis Procedures are reviewed and evaluated on an annual basis	Reduce risk	Low	Yes

Biometric data is recorded without consent	Procedures in place to ensure a valid consent form is held before the data is recorded. Procedures are reviewed and evaluated on an annual basis Staff training on data protection in place	Reduce risk	Low	Yes

Step 7: Sign off and record outcomes

Item	**Name/position/date**	**Notes**
Measures approved by:	Emma Gritten CFO 27 May 2025	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Emma Gritten CFO 27 May 2025	Consultation with ICO not required as no residual high risk
DPO advice provided:	Richard Maskrey Data Protection Officer 30 May 2025	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Data processing complies with the GDPR and DPA 2018 and can continue. Protection of Biometric Information Policy and DPIA effectively identify and mitigate potential risks to data subjects. Measures identified in step 6 of DPIA reduce all residual risks to low levels.		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		

Consultation responses reviewed by:	N/A	If your decision departs from individuals' views, you must explain your reasons
Comments: No formal consultation undertaken		
This DPIA will kept under review by:	Emma Gritten CFO	The DPO should also review ongoing compliance with DPIA