Data Protection Impact Assessment
(Iris Biostore Cashless Catering)

Bishop Milner Catholic College operates an automated biometric recognition system which uses biometric information about pupils. The Protection of Freedoms Act 2012 placed a duty on schools and colleges to process biometric information about pupils in a specific way and as such Bishop Milner Catholic College must consider the privacy implications of such a system. Protection of biometric information of children in schools and colleges to process biometric information about pupils in a specific way can be viewed at this link. The Data Protection Impact Assessment is a systematic process for identifying and addressing privacy issues and considers the future consequences for privacy of a current or proposed action.

The processing of biometric information means any operation or set of operations which is performed on personal data including obtaining, recording and storing the pupils' data on a database system. In terms of Iris Biostore Cashless Catering this involves the taking of measurements of a finger print (biometric information).

The current on-prem solution does not store any data in the cloud. All data is stored locally within the schools network and infrastructure.

Bishop Milner Catholic College recognises that moving to a biometric based solution has a number of implications. Bishop Milner Catholic College recognises the need to have a good overview of its data information flow. The completion of the Data Protection Impact Assessment highlights some of the key implications.

The Data Protection Impact Assessment looks at the wider context of privacy taking into account Data Protection Law and the Human Rights Act. It considers the need for a biometric based data system and the impact it may have on individual privacy. The Data Protection Impact Assessment helps determine whether the proposed system can be justified as proportionate to the needs of the school.

Bishop Milner Catholic College recognizes that changes do occur and on this basis good practice recommends that the school review its Data Protection Impact Assessment.

A Data Protection Impact Assessment will typically consist of the following key steps:

1. Identify the need for a DPIA.
2. Describe the information flow.
3. Identify data protection and related risks.
4. Identify data protection solutions to reduce or eliminate the risks.
5. Sign off the outcomes of the DPIA.

Contents

Step 1: Identify the need for a DPIA

What is the aim of the project? – To help deliver a cost effective solution to the needs of the business. Iris Biostore Cashless Catering supports and improves hygiene and simplifies financial operations with online payments. It eliminates cash and enables users to pay utilising either fingerprint, pin code or ID card. It enables integration between the cashless catering and the school's identity management database providing a complete overview of user attendance, payments and more. It also improves kitchen operations with advanced meal selection, stock control, supplier management and reporting

Iris Biostore Cashless Catering is the school's meal management module which can achieve the following:

Pre order meals using interactive whiteboards – It is simple and quick to use for both pupils and teachers, the interactive whiteboard meal pre-order and attendance screen gathers the information the kitchen needs for food preparation, driving efficiency and reducing costs.

Cashless Vending – Managing school dinner money payments effectively significantly reduces the school administration of handling cash and provides accurate monitoring of free school meal eligibility with full audit trails.

Parents can pre-order and pay online – IRIS FasTrak uses a web based payment portal that enables parents to pre-order and make secure online payments for their child's school meals, without the need to send cash to school. Parents can log in to view available meal options for weeks ahead

Managing payments for school meals – Managing school dinner money payments effectively will significantly reduce the school administration of handling cash and provide accurate monitoring of free school meal eligibility with full audit trails.

It enables an effective and efficient delivery of catering services to the end user.
Bishop Milner Catholic College will undertake the following processes:

1. Identifying and obtaining biometric information
2. Recording biometric information
3. Organising biometric information
4. Storing & deleting biometric information
5. Disclosing biometric information
6. Automation of biometric information (biometric data and pupil)

By opting for a biometric based solution the school aims to achieve the following:

- Efficiency of service delivery
- Reliability
- Resilience in meeting high volume requirements
- Delivery at a potentially lower cost

Step 2: Describe the processing

Bishop Milner Catholic College must notify each parent of a pupil under the age of 18 if they wish to take and subsequently use the child's biometric data as part of an automated biometric recognition system. The Protection of Freedoms Act guidance states the parents of a child include not only the biological mother or father (or the adoptive parents) but any other individual with parental responsibility for the child. Part 1 of the Children Act 1989 sets out who has parental responsibility and what this means.

The use of biometric data is recorded in the school's Privacy Notice (Pupil). It also states that parental consent must be obtained and recorded separately. This would include informing the parent what the system is, why it is being used and the biometric information obtained.

There will never be any circumstances in which Bishop Milner Catholic College can lawfully process a child's biometric information (for the purposes of using an automated biometric recognition system) without having written consent. The nature of processing is as follows:

Identifying and obtaining biometric information – Iris Biostore Cashless Catering software products hold personal data sourced from the school's Management Information System. The pupil data is required to verify the identity of the individual at the point of service delivery.

Commonly held data includes pupil surname, forename, registration group, year, date of birth, gender, free meal eligibility, admission number, Management Information System Identification (MISID), photograph, card number, and biometric (fingerprint) template.

Recording biometric information – Biometric data (fingerprints) are stored as a series of data points, converted from images by a mathematical algorithm. This is comprised of between ten and sixty depending on the characteristics of the finger. This is then encrypted and stored as a template. These data points cannot be used to reconstruct a useable fingerprint even with the algorithm available.

Organising biometric information – Data is held in software database tables held securely within the school. The current on-prem solution does not store any data in the cloud. All data is stored locally within the school's network and infrastructure.

The data is held on a server with folder permissions restricted and/or controlled by user/group permissions. These are configured to allow/deny users access to view/edit individual fields and reports. User logins and passwords plus biometric data is encrypted.

Bishop Milner Catholic College as data controller is responsible to determine what access individual users should be allowed.

Storing & Deleting biometric information – The data points are encrypted before being stored. The encryption standard used for encrypting the data points is AES 256 with the symmetric key being stored in RSA 2048. The AES 256 encryption standard is used for storing top secret designated data by the American military and the NSA. Both AES and RSA are well used and commonly understood encryption standards that cannot be broken by brute force in a reasonable time.

Bishop Milner Catholic College as data controller is responsible to ensure that data is not retained for "longer than is necessary." Iris Biostore Cashless Catering software products typically archive on an annual basis. This data is available to be reported on until
Bishop Milner Catholic College decides it is no longer. Information is deleted either manually or through a daily update provided through the school's Management Information System. The school also reviews its data on an annual basis.

Disclosing biometric information – UK GDPR gives the right to individuals to access their personal data and supplementary information held about them. Iris Biostore Cashless Catering intend to make a tool available which allows all data to be supplied in a single report to help satisfy subject access requests.

Automation of biometric information with the pupil – The information obtained will be for the use of automated biometric recognition and for no other purpose and will not be shared with any other system. The information collected by the school is retained on the school's management biometric based data system. The information is retained according to the school's Data Retention Policy.

Bishop Milner Catholic College collects and processes biometric data relating to its pupils to support its automated biometric recognition system.

Article 4 of the General Data Protection Regulation defines biometric information as 'personal data' resulting from specific technical processing relating to physical, physiological or behavioral characteristics of a natural person which allow or confirm the unique identification of the natural person.'

What is the nature of the data? – Fingerprint data stored as a series of data points, converted from images by a mathematical algorithm. This is comprised of between ten and sixty depending on the characteristics of the finger. These data points cannot be used to reconstruct a useable fingerprint even with the algorithm available. This is then encrypted and stored as a template.

Special Category data – Biometric data is defined as 'special category' personal information under the General Data Protection Regulation. Under Data Protection Law it is a mandatory requirement to undertake a Data Protection Impact Assessment.

How much data is collected and used and how often? – Consent is obtained from those that have parental responsibility for the pupil. The consent is obtained as a one-off. Biometric information will be used on the system for only those pupils where consent has been obtained.

How long will you keep the data for? – Biometric data is kept from the point of entry to the point of exit during the school life of the pupil at Bishop Milner Catholic College. Once the biometric information is no longer needed this is deleted securely. This information is contained within the school's Privacy Notice and also forms part of the notification of intention to process pupils' biometric information consent form.

Scope of data obtained? – Consent has been obtained for Year 7 pupils once they have attained a place at Bishop Milner Catholic College. The pupil data is registered in advance from the Management Information System and the biometric information is obtained from the pupil. This is cross referenced by class group with the consent obtained for the relevant pupil.

The Privacy Notice includes information about the processing of the pupil's biometric information that is sufficient to ensure that parents are fully informed about what is being proposed. The Privacy Notice includes the following:

- Contact details of the organization using biometric data;
- Details about the type of biometric information to be taken;
- How it will be used;
- Any retention periods';
- School's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed

Access to the management information system which uses biometric data will be controlled by username and password.

The school provides education to its students with staff delivering the National Curriculum.

The use of biometric information is a novel technology and is used in schools to borrow library books, for cashless canteen systems, vending machines, recording class attendance and payments into schools.

Bishop Milner Catholic College recognises that moving to a biometric based solution raises a number of General Data Protection Regulations as follows:

- ISSUE: The management information system will be storing biometric data 'special category' information
  RISK: There is a risk of obtaining biometric data for other purposes
  MITIGATING ACTION: Biometric data (fingerprints) are stored as a series of data points, converted from images by a mathematical algorithm. This is comprised of between ten and sixty depending on the characteristics of the finger. 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. The data points are encrypted before being stored. The encryption standard used for encrypting the data points is AES 256. Each school has its own unique set of encryption keys.

For the Biostore Cashless Catering Payment System only

- ISSUE: Iris Biostore Cashless Catering (online payment system)
  RISK: There is a risk of unauthorized access to information by third parties
  MITIGATING ACTION: The following controls are in place. (1) Iris Biostore Cashless Catering log data around login attempts which includes failures and origin IP addresses. (2) They have protections against someone attempting to access an account that doesn't belong to them. (3) It should be noted, the source IP address is not a consideration in determining the validity of a login request. (4) Additionally, all traffic is inspected in real time using an IDS solution – suspicious activities are blocked and reported. (5) Iris Biostore Cashless Catering use industry-standard security practices and run frequent audits to ensure their systems are secure and data is kept safe

For the Biostore Cashless Catering Payment System only

- ISSUE: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred. MITIGATING ACTION: All data transfers are done using secure methods (such as data being encrypted when transferring data to and from Iris Biostore Cashless Catering web servers)

For the Biostore Cashless Catering Payment System only

- ISSUE: Cloud solution and the geographical location of where the data is stored
  RISK: Within the EU, the physical location of the cloud is a decisive factor to determine which privacy rules apply. However, in other areas other regulations may apply which may not be Data Protection Law compliant
  MITIGATING ACTION: All data is stored on UK servers on private cloud infrastructure. Where data is stored in the UK this means that the UK GDPR privacy rules apply to the cloud based service

- ISSUE: The management information system will be storing biometric data 'special category' information
  RISK: There is a risk of uncontrolled distribution of information to third parties. MITIGATING ACTION: Access to data is controlled by user/group permissions. These can be configured to allow/deny users access to view/edit individual fields and reports. It is the school, data controller's, responsibility to determine what access individual users should be allowed

  The data controller will ensure that the software database tables are held securely within the school. This includes ensuring the server on which it is being stored has up to date anti-virus software, is in a physically secure location and folder permissions are restricted to authorised users

- ISSUE: Use of third party sub processors?
  RISK: Non-compliance with the requirements under UK GDPR
  MITIGATING ACTION: Where possible, IRIS will choose suppliers, vendors and sub-processors that can guarantee personal data will not be transferred to or accessible from third countries unless that territory meets the European Essential Guarantees requirements. Where a supplier, vendor or sub-processor cannot provide the guarantee described IRIS will either (1) pseudonymise the personal data prior to transfer so that it is not possible for any identification of individuals to take place in a third country, or (2) encrypt the personal data before transfer so that IRIS retains the encryption keys and so it is not possible for identification of any individuals to take place in a third country. IRIS will ensure that the relevant Model contract clauses to safeguard personal data

transferred to third countries and territories are included in supplier data processing agreements

- ISSUE: Data Ownership
  RISK: The school must maintain ownership of the data
  MITIGATING ACTION: Iris Biostore Cashless Catering is the data processor and the school is the data controller

- ISSUE: Subject Access Requests
  RISK: The school must be able to retrieve the data in a structured format to provide the information to the data subject. Typically, an image would not be retained but the system may store plotted positions of facial features or fingerprint grid locations. It would be the case that these numerical values are personal data if and when associated with other data held
  MITIGATING ACTION: IRIS will ensure it has the processes and procedures in place within its Group systems and products to manage the rights of individuals, including:
  (a) Right of an individual to have access to personal information IRIS holds about them
  (b) Right to rectification of inaccurate personal information
  (c) The limited right to erasure (right to be forgotten)
  (d) Right to restriction of use of an individual's personal information
  (e) Right to data portability
  (f) Right to object
  (g) Right to know about automated individual decision-making and profiling.

- ISSUE: Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: After the end of service provision, IRIS will delete or return all the personal data to the customer in line with customer's choice and will permanently delete existing copies unless the law requires IRIS to continue storage for a specified time. In the latter case, IRIS will identify the specific legislation that required IRIS to hold the data for a longer period and will ensure processes are in place to dispose of the data at the end of that retention period

- ISSUE: Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Iris Data Protection Policy states that all staff must follow the corporate procedure for reporting personal data breaches (and allegations of breaches) to the Group Data Protection Offer without delay. Incidents must immediately be reported by a call (Teams or phone) to the Group Data Protection Officer in addition to any written report about the incident. The full corporate procedure is published to all staff on the MetaCompliance platform

IRIS will inform customers without delay of any personal data breach affecting a customer's data and will assist in providing information required for notification to the relevant regulator and affected data subjects where necessary

- ISSUE: Post Brexit
  RISK: UK GDPR non-compliance.
  MITIGATING ACTION: Iris Biostore Cashless Catering is stored on the schools local servers and linked to the schools Management Information System

- ISSUE: Consent is not given by the parent or legal guardian
  RISK: The pupil is excluded from the service provided
  MITIGATING ACTION: Alternative arrangements are put in place to ensure the pupil does not suffer any disadvantage or difficulty in accessing services. This is a PIN number which is registered against the management information system and issued to the pupil. These arrangements do not place any additional burden on parents whose children are not participating in the scheme

- ISSUE: UK GDPR Training
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Appropriate training is undertaken by personnel that have access to Iris Biostore Cashless Catering

- ISSUE: Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Biometric information is housed on a dedicated server which does not integrate with any other server. Access to the data for on-prem solutions is controlled by the school themselves as data controllers. Any access granted to the system would be done so under the control of the school. Individual permissions can be set within each of the applications to restrict the users access for that application or data within.

The information is encrypted. The biometric data is backed up to a mirror server

The school moving to a system using biometric data will realise the following benefits:

- Efficiency of service delivery
- Reliability
- Resilience in meeting high volume requirements
- Delivery at a potentially lower cost

Step 3: Consultation process

The views of senior leadership team and the Board of Governors will be obtained along with parents and pupils. Once reviewed the views of stakeholders will be taken into account.

The view of YourIG has also been engaged to ensure Data Protection Law compliance.

Step 4: Assess necessity and proportionality

What is the lawful basis for processing? - The lawful basis for processing biometric data is obtained through explicit consent from those who have parental responsibility for the pupil. This lawful basis is recorded in the school's Privacy Notice.

Does the processing achieve your purpose? – Enables the pupils to access school services in an efficient and cost effective manner.

Is there another way to achieve the same outcome? – The delivery of the service is time dependent and the volume of pupils using the service necessitates the need to use a system which can meet the demands of a high volumes.

How will you prevent function creep? – Schools using automated biometric recognition systems must notify parents and obtain consent. There are no circumstances in which a school can lawfully process a pupil's biometric data without receiving the necessary consent.

How will you ensure data quality and data minimisation? – Iris Biostore software products hold personal data sourced from the school's Management Information System. Data includes pupil surname, forename, registration group, year, date of birth, gender, free meal eligibility, admission number, MISID, photograph, card number, and biometric (fingerprint) template. The information will only be used to deliver the service to the end user.

What information will you give the individuals? – The school has a Subject Access Request procedure in place to ensure compliance with Data Protection Law.

How will you help them support their rights? – Iris Biostore to provide the technical capability to ensure the school can satisfy data subject access requests supporting the data subjects right to be informed; the right of access; the right of rectification; the right to erasure; the right to restrict

processing; the right to data portability; the right to object; and the right not to be subject to automated decision-making.

The school will continue to be compliant with its Data Protection Policy.

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**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Storing of biometric information	Possible	Significant	Medium
Third party access	Possible	Significant	Medium
Data Ownership	Possible	Significant	Medium
Subject Access Request	Possible	Significant	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**
		Eliminated reduced accepted	Low medium high	Yes/no
Data security	User name and password.	Reduced	Medium	Yes
Data storage	Data stored as an algorithm and encrypted	Reduced	Low	Yes
Data Ownership	School retains ownership and documented in contract	Reduced	Low	Yes
Subject Access Request	Technical capability to satisfy data subject access request	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Siobhan Foster	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Siobhan Foster	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Yes	DPO should advise on compliance, step 6 measures and whether processing can proceed

Summary of DPO advice:

YourIG has sort clarification on the following:

(1) Iris Biosphere's Data Protection Policy makes reference to information being store in the cloud. Does this include biometric information as part of the cashless catering system?

(2) The Iris Biostore will be storing biometric data 'special category' information. There is a risk of obtaining biometric data for other purposes. What security measures are put in place to mitigate against this risk? (i.e. is the biometric data (fingerprints) stored as a series of data

points, converted from images by a mathematical algorithm? Are these data points encrypted before being stored? What is the encryption standard used for encrypting the data points?

(3) How is access to data controlled? Is it by user/group permissions? How are these configured? Is it the school, data controller's, responsibility to determine what access individual users should be allowed?

(4) As part of the Iris Biostore Cashless Catering will the online payment system be stored in the cloud? In terms of both the cashless catering (if applicable) and the online payment system

(a) Is there monitoring in place for unusual activity, for example attempted access from unrecognised IP addresses, or failed log in attempts?
(b) Are databases encrypted at rest using AES and 3DES encryption algorithms; and are there firewalls in place to maximise security?
(c) What securities are in place when transferring data between the school and the cloud? Is data encrypted during transit?
(d) Confirmation that personal data is stored on UK servers. If elsewhere, have model contract clauses been used, etc?

The response from the third party DPO has been included as part of the issues, risk and mitigating actions log in step 2 of this DPIA

DPO advice accepted or overruled by If overruled, you must explain your reasons
Comments:
Consultation responses reviewed by: If your decision departs from individuals' views, you must explain your reasons
Comments

This DPIA will kept under review by:	Gabriela Roden	The DPO should also review ongoing compliance with DPIA