STUART BATHURST CATHOLIC HIGH SCHOOL

Data Protection Impact Assessment (Biometrics)

Data Protection Impact Assessment (Biometric)

Stuart Bathurst Catholic High School 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 Stuart Bathurst Catholic High School 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.

An automated biometric recognition system uses technology which measures an individual's physical or behavioral characteristics by using equipment that operates automatically, i.e. electronically. Stuart Bathurst Catholic High School recognises that moving to a biometric based solution has a number of implications. Stuart Bathurst Catholic High School 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. Stuart Bathurst Catholic High School recognises that changes do occur and, on this basis, good practice recommends that the school review its Data Protection Impact Assessment.

What is the aim of the project?

To help deliver a cost-effective solution to the needs of the business, e.g. the use of biometrics for catering purposes means that pupils do not need to bring money into school

The processing of biometric information means any operation or set of operations which is performed on personal data including obtaining, recording, e.g. taking measurements of a finger print, storing data, e.g. storing pupils' biometric information on a database system.
Stuart Bathurst Catholic High School 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

Stuart Bathurst Catholic High School 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 Stuart Bathurst Catholic High School 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:
Stuart Bathurst Catholic High School collects and processes biometric data relating to its pupils to support its automated biometric recognition system.

Article 4 of the UK 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?

Finger prints, facial shape, retina and iris patterns, and hand measurements

Special Category data

Biometric data is defined as 'special category' personal information under the UK 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?

Extent of data collected, i.e. all pupils or only pupils subscribing to a service? Is the data collected as a one off?

How long will you keep the data for?

Consider the data retention period and how long the information needs to be retained. Is this included in the Privacy Notice? Is it incorporated within the school's Data Retention Policy?

Scope of data obtained?

How many individuals are affected, i.e. Year 1 pupils? And what is the geographical area covered; i.e. Year 1 pupils within Stuart Bathurst Catholic High School
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.

Stuart Bathurst Catholic High School recognises that moving to a biometric based solution raises a number of UK 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 uncontrolled distribution of information to third parties. **MITIGATING ACTION:** Consider the use of an authentication process, for example, using a username and password system

- **ISSUE:** Lawful basis for processing personal data
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: School has included IRIS BioStore Ltd in its Privacy Notice (Pupil), (Workforce), and (Governors and Volunteers) which identifies the lawful basis for processing personal data. The lawful basis is based on Article 6 1 (a) "the data subject has given consent to the processing of his or her personal data for one or more specific purposes"

- **ISSUE:** Data Ownership
  RISK: The school must maintain ownership of the data
  MITIGATING ACTION: This should be included in the contract with any third-party organisation

- **ISSUE:** Data Retention
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: School to take into consideration backups and if the data is stored in multiple locations and the ability to remove the data in its entirety

- **ISSUE:** Responding to a Data Breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school will recognize the need to define in their contract a breach event and procedures for notifying the school and the school managing it

- **ISSUE:** Third party processor and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: The school is unable to exercise the rights of the individual
  MITIGATING ACTION: IRIS BioStore Ltd will need to provide the technical capability to ensure the school can comply with such requests. This may be included as part of the contract

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: What does the third-party processor intend to do to allow data processing in the UK to remain compliant

- **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: Providers will need to provide the technical capability to ensure the school can satisfy data subject access requests

- **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. Additionally, such arrangements should not place any additional burden on parents whose children are not participating in the scheme.

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school must assess what kind of security and privacy measures are in place. Cloud providers can demonstrate compliance through a DPIA, being ISO 27001 certified, etc

  If cloud based the following applies:

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred.
  MITIGATING ACTION: Encryption ensures data 'in transit' between endpoints should be secure and protected from interception. This can be achieved by using an encrypted protocol or other secure methods

- **ISSUE:** Cloud Architecture
  RISK: The school needs to familiarise itself with the underlying technologies the cloud provider uses and the implications these technologies have on security safeguards and protection of the personal data stored in the cloud.
  MITIGATING ACTION: This should be monitored to address any changes in technology and its impact on data. The school should maintain ownership of the Cloud technologies used ensuring current and future technologies enable UK GDPR compliance

- **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: To determine the privacy rules which apply based on the location of the cloud

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: It is advisable that the school tailor any contract to incorporate these privacy commitments

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

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.

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?

Consider the source of the data? It is accurate but how is it kept up to date? Is the information adequate, relevant and limited to what is necessary?

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?

How can the management information system support the rights of the data subject? Does it have the capability to achieve the following: the 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.

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 and third-party access	Possible	Severe	Medium
Data Ownership	Possible	Significant	Medium
Post Brexit (GDPR noncompliance)	Possible	Significant	Medium
Subject Access Request	Probable	Significant	Medium

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 storage	User name and password	Reduced	Medium	Yes
Data Ownership	School retains ownership and documented in contract	Reduced	Low	Yes
Post Brexit	Contingency plans in place	Reduced	Low	Yes
Subject Access Request	Technical capability to satisfy data subject access request	Reduced	Low	Yes

Item	Name/date	Notes
Measures approved by:	Richard May	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Richard May	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	No	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
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:	Alicia Mortimer	The DPO should also review ongoing compliance with DPIA