Data Protection Impact Assessment (Cunninghams Cashless Catering)

The Earls 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 [insert Name of 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.

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 Cunninghams Cashless Catering the taking of measurements of a finger print (biometric information).

The Earls High School recognises that moving to a biometric based solution has a number of implications. The Earls 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.

The Earls High School 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

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.

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. It also enables an effective and efficient delivery of catering services to the end user.

The Earls 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

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 Earls 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 [insert Name of 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:

Identifying and obtaining biometric information – CRB Cunninghams 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. 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 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.

The Earls High School 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.

The Earls High School as data controller is responsible to ensure that data is not retained for "longer than is necessary." CRB Cunninghams software products typically archive on an annual basis. This data is available to be reported on until [insert Name of School] 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. CRB Cunninghams 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.

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 Earls High School 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. These data points cannot be used to reconstruct a useable fingerprint even with the algorithm available.

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 The Earls High School. 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 The Earls High School. 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.

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)?

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.

The Earls High School 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. 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 with the symmetric key being stored in RSA 2048

- **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:** Data Ownership
  RISK: The school must maintain ownership of the data
  MITIGATING ACTION: Cunninghams 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: Cunninghams Cashless Catering is able to provide the technical capability to ensure the school can satisfy data subject access requests.

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance.
  MITIGATING ACTION: Cunninghams 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 swipe card 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 Cunninghams 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. The information is encrypted. The biometric data is backed up to a mirror server. Cunninghams Cashless Catering is ISO 27001 accredited

  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 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

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 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

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?

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? – CRB Cunninghams 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? – Cunninghams Cashless Catering 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:	Jamie Fox	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Jamie Fox	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:

(1) Access to data and implementation of appropriate user/group permissions?
By secure login and password for staff and remotely for parents.

(2) What are the alternative arrangements for those where parental consent is not given
Cash cards can be obtained by students.

(3) Data ownership and maintaining ownership
Owned by school

(4) What is the data retention period, how long does information need to be retained?
Authorized data retained for full time student is in school then deleted once they leave school

(5) How will the information be deleted securely?
In line with supplier instructions at academic year end

DPO advice accepted or overruled by: No

If overruled, you must explain your reasons

Comments:

Above

Consultation responses reviewed by: n/a as staff and parents have other options available if they do not wish to use the system, parents of new students joining in year 7 have to give permission to use system.

If your decision departs from individuals' views, you must explain your reasons

Comments: [Comments provided]		
This DPIA will kept under review by:	Anna Wade	The DPO should also review ongoing compliance with DPIA