Summerhill School

Data Protection Impact Assessment - Papercut

Summerhill School operates an automated biometric recognition system which uses biometric information about students. The Protection of Freedoms Act 2012 placed a duty on schools and colleges to process biometric information about students in a specific way and as such Summerhill 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 students 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.

Summerhill School recognises that moving to a biometric based solution has a number of implications. Summerhill 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.

Summerhill School recognises 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.

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 students 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 students' biometric information on a database system. Summerhill 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 student) 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?

Summerhill School must notify each parent of a student 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 (Student). It also states that parental consent must be obtained and recorded separately. This includes 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 Summerhill 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 – Summerhill school will collect a fingerprint as a source of biometric information.

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 securely within the school. The data is held on a server with folder permissions controlled by user permissions.

Storing & deleting biometric information – Information is stored on the server within a database. Summerhill school as data controller is responsible to ensure data is not retained for 'longer than necessary'. Information is then deleted.

Disclosing biometric information – GDPR gives the right to individuals to access their personal data and supplementary information held about them.

Automation of biometric information with the student –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?
Summerhill School collects and processes biometric data relating to its students 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. **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?** – Fingerprints are collected from all staff and students once they start at Summerhill school. Fingerprints are only collected again if a subject's fingerprint is not being recognised reliably by the system. Two fingerprints are collected from each person (usually one from each hand, to provide an alternative in case of an injury to either hand) **How long will you keep the data for?** – Biometric data is kept from the point of entry to Summerhill school to the point of exit during the school life of the member of staff / student. Once this is no longer needed it is deleted. This information is also contained within the school's Privacy Notice and also forms part of the notification of intention to process students' biometric information consent form. **Scope of data obtained?** – There are 1100 staff / students at Summerhil School. The Privacy Notice includes information about the processing of the student'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 organisation 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 students 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.

Summerhill 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 uncontrolled distribution of information to third parties.
  MITIGATING ACTION: We use an authentication system, using a username and password system

- **ISSUE:** Data Ownership
  RISK: The school must maintain ownership of the data
  MITIGATING ACTION: School does maintain ownership of the data. There is currently no transfer of data to a third party for the purposes of Papercut, as all processing is done by the school. If such a transfer were to be introduced, the contract would include that the school retained ownership of the data

- **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: The software provides 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 student is excluded from the service provided
  MITIGATING ACTION: Where consent to use biometric information is not given, students will use their network email address and password to log into printers to access the printing system.

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
- Access for staff and students without the need to remember additional authorisation codes or carry additional forms of authorisation

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 biometric system is well established at Summerhill School, with consent having been obtained for the gathering of all existing biometric data.

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 student. This lawful basis is recorded in the school's Privacy Notice. **Does the processing achieve your purpose?** – Enables the students 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 students 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 student's biometric data without receiving the necessary consent **How will you ensure data quality and data minimisation?** – At the time that fingerprint data is first collected, each finger is scanned until a consistent recognition pattern is obtained. Scanning two fingers per individual is the minimum number that will adequately provide a robust system which can function in the case of an injury to one hand. Fingerprint data should usually remain unchanged throughout an individual's time at Summerhill School, but fingerprints will be re-scanned if an individual's fingerprint should change for any reason. **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?** –RM 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 and third party access	Possible	Severe	Medium
Data Ownership	Possible	Significant	Medium
Subject Access Request	Probable	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 storage	User name and password	Reduced	Medium	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:	Adrian Cresswell	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Adrian Cresswell	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:		
DPO advice accepted or overruled by:	Yes	If overruled, you must explain your reasons
Comments: **[DPO Advice provided]**		
Consultation responses reviewed by:	**[Insert name]**	If your decision departs from individuals' views, you must explain your reasons
Comments: **[Comments provided]**		
This DPIA will kept under review by:	Vicki Poole	The DPO should also review ongoing compliance with DPIA