

# Biometrics in Schools, Colleges and other Educational Institutions

The following guidance has been prepared as an aid to schools, colleges and other educational institutions that may be considering the installation and use of a biometric system. This document is intended to encourage such institutions to fully consider if there is need for a biometric system in the first place and then to assess the privacy impact of different systems.

**The critical issues to be considered from a data protection perspective are the proportionality of introducing a biometric system and the requirement to obtain the signed consent of the student users (and their parents or guardians in the case of minors) giving them a clear and unambiguous right to opt out of the system without penalty.**

The document is not intended to promote any particular system, but is intended to make schools and colleges aware of their responsibilities under the Data Protection Acts 1988 & 2003. It is the use of a biometric system that may give rise to a data protection concern, not necessarily the production or sale of a system. All situations must be judged on a case-by-case basis.

## 1. Different types of Biometric systems

All biometric systems operate on the basis of the automatic identification or authentication/verification of a person. What differs between systems is the nature of the biometric and the type of storage.

### 1.1 Information used to generate biometric data

Biometric data may be created from physical or physiological characteristics of a person. These include a fingerprint, an iris, a retina, a face, outline of a hand, an ear shape, voice pattern, DNA, and body odour. Biometric data might also be created from behavioural data such as hand writing or keystroke analysis. Generally, a digitised template is produced from the biometric data. This template is then compared with one produced when a person presents at a reader.

### 1.2 Types of biometric data

There are three principal types of biometric data:

- Raw Images, consisting of recognisable data such as an image of a face or a fingerprint, etc.
- Encrypted images, consisting of data that can be used to generate an image.
- Encrypted partial data, consisting of partial data from an image, which is encrypted and cannot be used to recreate the complete original image.

### 1.3 Types of Biometric systems

There are two principal types of systems:

- Identification systems, which confirm the identity of an individual;
- Authentication / verification systems, which confirm that a biometric derived from a person who presents at a reader matches another biometric, typically stored on a card and presented simultaneously.

## 1.4 Storage of biometric data.

There are two principal methods of storing biometric data/templates:

- Central databases store the templates on a central system which is then searched each time a person presents at a reader.
- A card is used to store a template. A template is generated when a person presents at a reader, and this template is compared with the template on the card.

## Data Protection issues concerning biometrics.

### 2. Proportionality

Section 2(1)(c)(iii) of the Data Protection Acts states that data

"shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed."

The key word here is "excessive." Accordingly, the first question to be asked when considering the installation of such a system is what is the need for it? What is wrong with current systems or less invasive alternatives?

As individuals have fundamental Human Rights which are protected by the Data Protection Acts, a school or college must conduct some assessment of the need for a biometric system and an evaluation of the different types of available systems before the introduction of any particular system.

Determining what is excessive requires a case-by-case analysis. Some factors which may be taken into account include:

- **Environment.** Does the nature of the school or college require high levels of security? Are there areas of the campus which contain sensitive information, high value goods or potentially dangerous material which may warrant a higher level of security than would areas with low value goods or areas with full public access? Of course such a consideration would also point towards all persons working in the environment being similarly required to use the biometric system.
- **Purpose.** Can the intended purpose be achieved in a less intrusive way? A biometric system used to control access for security purposes in certain areas of the campus might be legitimate while a biometric system used by the same school or college purely for attendance management purposes might not.
- **Efficiency.** Ease of administration may necessitate the introduction of a system where other less invasive systems have failed, or proved to be prohibitively expensive to run.
- **Reliability.** If a school or college suffers as a result of students impersonating each other for various reasons, then a system could possibly be justified as long as other less invasive ones have been assessed and reasonably rejected.

### 3. Fair obtaining and processing.

Section 2(1)(a) of the Acts require that

"The data or, as the case may be, the information constituting the data shall have been obtained, and the data shall be processed, fairly."

In order to demonstrate compliance with this provision, at least one of the provisions of Section 2A of the Acts must be met. In the context of the introduction of a biometric system for use by students in a school or college, these include:

- Consent, and
- Legitimate interests of the school or college: where the processing is necessary for the purposes of the legitimate interests pursued by the school or college or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

**Consent:** In the context of students attending a place of education, the Data Protection Commissioner would stipulate that the obtaining of consent is of paramount importance when consideration is being given to the introduction of a biometric system. It is the Commissioner's view that when dealing with personal data relating to minors, the standards of fairness in the obtaining and use of data, required by the Data Protection Acts, are much more onerous than when dealing with adults. Section 2A(1)(a) of the Data Protection Acts states that personal data shall not be processed by a data controller unless the data subject has given his/her consent to the processing, or if the data subject by reason of his/her physical or mental incapacity or age, is or is likely to be unable to appreciate the nature and effect of such consent, it is given by a parent or guardian etc. While the Data Protection Acts are not specific on what age a subject will be able to consent on their own behalf, it would be prudent to interpret the Acts in accordance with the Constitution. As a matter of Constitutional and family law a parent has rights and duties in relation to a child. The Commissioner considers that use of a minor's personal data cannot be legitimate unless accompanied by the clear signed consent of the child and of the child's parents or guardian.

As a general guide, a student aged eighteen or older should give consent themselves. A student aged from twelve up to and including seventeen should give consent themselves and, in addition, consent should also be obtained from the student's parent or guardian. In the case of children under the age of twelve, consent of a parent or guardian will suffice. All students (and/or their parents or guardians as set out above) should, therefore, be given a clear and unambiguous right to opt out of a biometric system without penalty. Furthermore, provision must be made for the withdrawal of consent which had previously been given.

**Legitimate interests:** Whilst the "legitimate interest" provision may seem appealing, it requires that a balance be struck. What is acceptable in one case may not be acceptable in another and a school or college seeking to rely upon this provision must take into account the potential effect upon student privacy rights. In any event, the Data Protection Commissioner considers that, in the context of a student environment, the processing of personal data using a biometric system would be prejudicial to the fundamental rights and freedoms of the students concerned in the absence of freely given consent.

### 3A. Fair obtaining of sensitive data.

If a biometric identifies sensitive data (such as data relating to a student's health or facial appearance thereby revealing race), at least one provision of section 2B of the Acts must be met in addition to those mentioned above. In the context of the introduction of a biometric system for use by students in a school or college, these provisions include:

- consent explicitly given.
- necessary processing for the performance of a function conferred on a person by or under an enactment.

Explicit consent: As stated above, all students (and/or their parents or guardians) should be given a clear and unambiguous right to opt out of a biometric system without penalty. The same consent which applied to the principle of obtaining and processing data fairly also applies to the fair obtaining of sensitive data.

Necessary for the performance of a function conferred under an enactment: Any legal obligation to record the attendance of students need not, in itself, require a biometric system to satisfy. For example, the Education (Welfare) Act, 2000 requires schools to maintain a record of the attendance or non-attendance on each school day of each student registered at the school. This requirement does not specify how the attendance data should be obtained. The key word in this provision of the Data Protection Acts concerning the processing of sensitive personal data is "necessary." It is the view of the Data Protection Commissioner that the processing of sensitive personal data through use of a biometric system is not necessary to meet the requirements of the Education (Welfare) Act, 2000 in respect of recording student attendance. There are several long established and successful alternative methods of recording student attendance at schools which do not require the processing of a student's sensitive personal data.

## 4. Transparency

Section 2D of the Acts require that a school or college provide at least the following information to students when processing their data:

- The identity of the data controller in the school or college.
- The purpose in processing the data.
- Any third party to whom the biometric data will be given.

It is essential that students are aware of the purpose for which the biometrics data will be processed. This means that a school or college must carefully think through any purpose or potential purpose. Is the system solely for attendance management purposes? Will it be used for access control? What are the consequences for the student concerned if there is an identified abuse of the system? Under what circumstances will management access logs created by the system?

Transparency is even more important where the biometric system does not require the knowledge or active participation of a student. A facial recognition system, for instance, may capture and compare images without that person's knowledge.

## 5. Accuracy

Section 2(1)(b) of the Acts require that data shall be

"Accurate and complete and, where necessary, kept up to date."

Any biometric system must accurately identify the persons whose data are processed by the system. If changes in physical or physiological characteristics result in a template becoming outdated, a procedure must be in place to ensure that the data are kept up to date.

## **6. Security**

The requirement, under section 2(1)(d), that a school or college has appropriate security measures in place to prevent the unauthorised access to, or the unauthorised alteration, disclosure or destruction of data would appear to promote the use of technological solutions such as encryption.

However, in deciding upon what constitutes an appropriate security measure, Section 2C details four factors that should be taken into account:

- The state of technological development.
- The cost of implementing such technology.
- The nature of the data being protected.
- The harm that might result through the unlawful processing of such data.

A minimum standard of security would include:

- Access to the information restricted to authorised staff on a 'need to know' basis in accordance with a defined policy.
- Computer systems should be password protected.
- Information on computer screens or manual files should be hidden from persons who are not authorised to see them.
- A back-up procedure for computer held data, including off-site back-up.
- Ensuring that staff are made aware of the school or college's security measures, and comply with them.
- Careful disposal of documents such as computer printouts, etc.
- The designation of a person with responsibility for security and the periodic review of the security measures and practices in place.
- Adequate overall security of the premises when it is unoccupied.
- Where the processing of personal data is carried out by a data processor on behalf of the school or college, a contract should be in place which imposes equivalent security obligations on the data processor.

## **7. Retention**

Section 2(1)(c)(iv) of the Data Protection Acts provides that data shall not be kept for longer than is necessary for the purpose. In the context of a biometric system in a school or college, it would be necessary to devise a retention policy in advance of the deployment of the system which clearly sets out the retention period which would apply to biometric data. The Data Protection Commissioner would expect that as soon as a student permanently leaves the school or college, his/her biometric data would be immediately deleted.

## **8. Privacy Impact Assessment.**

The Data Protection Commissioner cannot give a general approval or condemnation of biometric systems. Each system must be judged in respect of the situation in which it is

used. A case-by-case judgement is required. With that in mind, the Commissioner encourages schools and colleges to take the above guidance into account if considering introducing any biometric system.

Before a school or college installs a biometric system, the Data Protection Commissioner recommends that a documented privacy impact assessment is carried out. A school or college which properly conducts such an assessment is less likely to introduce a system that contravenes the provisions of the Data Protection Acts 1988 & 2003. This is an important procedure to adopt as a contravention may result in action being taken against a school or college by the Commissioner, or may expose a school or college to a claim for damages from a student. Data protection responsibility and liability rests with the school or college, not with the person who has supplied the system (where that person also acts as a data processor on behalf of the employer, it will have its own separate data protection responsibilities in relation to the security of the data).

Some of the points that might be included in a Privacy Impact Assessment are:

- Do I have an attendance management and/or access control system in place?
- Why do I feel I need to replace it?
- What problems are there with the system?
- Are these problems a result of poor administration of the system or an inherent design problem?
- Have I examined a number of types of system that are available?
- Will the non-biometric systems perform the required tasks adequately?
- Do I need a biometric system?
- If so, which kind do I need?
- Do I need a system that identifies students as opposed to a verification system?
- Do I need a central database?
- If so, what is wrong with a system that does not use a central database?
- What is the biometric system required to achieve for me?
- Is it for attendance management purposes and/or for access control purposes?
- How accurate shall the data be?
- What procedures are used to ensure accuracy of data?
- Will the data require updating?
- How will the information on it be secured?
- Who shall have access to the data or to logs?
- Why, when and how shall such access be permitted?
- What constitutes an abuse of the system by a student?
- What procedures shall I put in place to deal with abuse?
- What legal basis do I have for requiring students to participate?
- How will I obtain the consent of the existing students (or their parents/guardians if applicable)?
- How will I obtain the consent of new students (or their parents/guardians) who will enrol at a future date?
- How will I ensure that students will be given a clear and unambiguous right to opt out of a biometric system without penalty?
- What procedures will I put in place to provide for the withdrawal by students of consent previously given?
- What system will I put in place for students who opt out of using the biometric system?
- How will I ensure that students who are unable to provide biometric data, because of a disability for example, are not discriminated against by my school or college by being required to operate a different system, or otherwise?

- Does the system used employ additional identifiers (e.g. PIN number, smart card) along with the biometric?
- If so, would these additional identifiers be sufficient on their own, rather than requiring operation in conjunction with a biometric?
- If the introduction of a biometric system is justified, can I offer an alternative system to individuals who may object to the invasion of privacy involved in a biometric system?
- What is my retention policy on biometric data?
- Can I justify the retention period in my retention policy?
- How shall I inform students about the system?
- What information about the system need I provide to students?
- Would I be happy if I was a student asked to use such a system?
- Am I happy to operate a biometric system in an educational establishment where the use of such a system can make students less aware of the data protection risks that may impact upon them in later life?
- Does my school or college have a comprehensive data protection policy as required by the Department of Education and Science since 2003?
- Have I updated this policy to take account of the introduction of a biometric system for use by students?