Becta guidance on biometric technologies in schools

Contents

1 Introduction – what this guidance is about

This guidance has been developed with support from the Department for Children, Schools and Families (DCSF) and in consultation with the Information Commissioner's Office (ICO). It is aimed primarily at headteachers, governing bodies and anyone else who may be involved in the process of introducing biometric technology into schools.

It is intended to provide headteachers and school governors with what they need to know about biometric technology systems if they are thinking of introducing such a system in their school, and to advise them on what steps they need to take to introduce it successfully.

The ICO has also set out its view on the use of biometric technology systems in schools. Its paper 'The use of biometrics in schools' can be accessed from the ICO website [http://www.ico.gov.uk].

Parents and carers may also wish to read the guidance, and the ICO's view, to help them understand what biometric technology is, what it can be used for, and what their rights are under relevant legislation.

2 What is biometric technology?

Everyone has physical or behavioural characteristics that are unique to them and change little over time. Fingerprints are a well-known example and (as is also well known) fingerprint details can be measured and recorded for subsequent identification purposes. There are other characteristics that can be used in this way, such as retina and iris patterns, voice, facial shape, hand measurements and behavioural characteristics such as handwriting and typing patterns.

Biometric technology describes the range of technologies used to measure, analyse and record one or more of these unique characteristics. The technology is generally used to support business processes which require confirmation of identity. Typically such processes involve:

- **registration** or authentication of identity (for example the recording of a fingerprint as belonging to Jane Doe)
- allocation of **entitlements** to people who have registered
- subsequent **verification** of identity (this person is indeed the Jane Doe who registered and who has the entitlement)
- and, sometimes, **identification** (this person is not in fact Jane Doe, but A.N. Other).

There are two approaches to recording an individual's biometric characteristics. The first is to record a complete image of, say, a face - as in a passport photograph or a fingerprint. The second is to take measurements that adequately capture the uniqueness of the source but do not capture a complete image. It is the second approach that is used in schools' biometric technology systems. With such an approach the original cannot be reconstructed from the data. It is not possible to recreate a pupil's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

3 School fingerprint recognition systems

Biometric systems currently used in schools are based on fingerprint recognition technology.

Manufacturers and suppliers of such systems state that their systems employ the second of the two approaches to capturing biometric details described above, storing numerical values derived from fingerprints and not actual images of fingerprints.

These systems work in the following way. A numerical value is derived from the child's fingerprint when it is first placed on the reading device. It is this numerical value which is then stored. Each time the child's fingerprint is subsequently re-read, a numerical value is again generated. This is compared with the set of stored values, uniquely identifying the child within the population of the school if a match is found. Schools do not keep an image of the fingerprint.

4 Examples of the use of biometric technology in schools

Biometric technology can underpin a range of systems supporting the efficient management and security of schools and other educational establishments. There follow some examples of such systems showing the role that biometric technologies can play in them. However such systems do not have to be supported by biometric systems. Other identification mechanisms (such as smartcards) can provide similar benefits. However, depending upon individual circumstances, biometric technologies can offer some additional advantages for schools. These are noted in each instance.

4.1 Example 1 – Cashless catering

School A uses a cashless catering system for school meals. Parents pay in advance for pupils' school lunches, crediting the pupils' accounts with the amount paid in. Pupils then use this credit to pay for their school lunches. Individual pupils are identified at the till by an automated mechanism, with the cost of their lunch being deducted from the credit paid for by the parent.

There are several advantages to cashless catering. Pupils in receipt of free school meals are not identifiable, which can help to avoid a pupil being stigmatised. In addition, pupils do not need cash to pay for their lunches, reducing the opportunity

for bullying and theft. Such systems can also speed up service in canteens and dining rooms.

In this instance, biometric technologies can offer some additional advantages over other identification mechanisms:

- Pupils do not need to remember to bring anything with them to the canteen and there is nothing that can be lost.
- Costs can be reduced as, for example, there is no requirement to replace lost or damaged smartcards.
- The risk of bullying and theft may be further reduced, as there is no opportunity for pupils to steal and use other pupils' smartcards to pay for meals.

4.2   Example 2 – Automated attendance and registration

School B uses an automated system for recording attendance. Pupils register via an automated mechanism at the school gate or entrance at the start and end of each day. Such systems can save considerable staff time and effort in taking registers. They can also help prevent unauthorised access to school premises.

School C takes this one step further by recording pupils' attendance at each class, so that truancy on the premises (which can be a problem in a large school) is recorded and can be dealt with, including by informing parents. The time spent while each pupil "keys in" for each class is minimal. Attendance data can also be used to help assess the impact of truancy on performance allowing any necessary steps to be implemented rapidly.

The advantages of employing biometric systems over other technologies are similar to those in the previous example. In addition, in this particular example, there is no opportunity for pupils to register absent pupils using their smartcards. Pupils must be physically present to register their attendance.

4.3   Example 3 – School library automation

School D uses biometric technology to help manage lending from the school library. An automated system identifies and records the pupil's name and the items they have borrowed or are returning. The advantages are similar to those outlined in the previous examples, in that,

- pupils do not need to remember to bring anything with them to use the library and there is nothing that can be lost, stolen or exchanged
- there is reduced opportunity for bullying and theft; pupils must be physically present to borrow items and cannot use another pupil's identity to do so.

5   The legal position and the Data Protection Act 1998

The governing body of a maintained school incorporated under section 19(1) of the Education Act 2002 has a power under paragraph 3(1) of Schedule 1 of that Act to

 "do anything which appears to them to be necessary or expedient for the purposes of, or in conjunction with (a) the conduct of the school, or (b) the provision of facilities or services under section 27 [of that Act.]"

This general enabling power clearly covers such matters as the introduction of biometric technology systems for purposes such as improving the administrative efficiency of the school.

In introducing and using such systems, schools must also comply with the Data Protection Act 1998. This is because the systems record biometric data – and that data must be treated just like any other personal data under the terms of the Act. What this means is set out more fully below, in sections 5.1 and 5.2.

5.1   Data Protection Act 1998

Schools hold personal data about pupils in order to run the education system effectively and, in so doing, must follow the requirements of the Data Protection Act 1998.

Schools are "data controllers" under the Act since they determine the purpose(s) for which and the manner in which any personal data is processed. Personal data is data which relates to individual pupils who can be identified from that data (or from that data and other information which the school holds). When personal data is obtained about pupils (who are the "data subjects") schools must ensure that the pupils and/or the parents (as appropriate – see section 5.2) are provided with a Fair Processing Notice which will contain information as to:

- the name of the data controller (the school)
- the purposes for which the data is held
- any information required to make the processing fair, including any third parties to whom the data may be passed.

In addition schools must comply with the following data protection principles which state that data must:

- be fairly and lawfully processed
- be processed for limited purposes
- be adequate, relevant and not excessive
- be accurate
- be kept no longer than necessary
- be processed in accordance with data subjects' rights
- be secure
- not be transferred to other countries without adequate protection of data subjects' rights.

As far as the Data Protection Act 1998 is concerned, biometric data must be handled in the same way as any other personal data and the same principles apply when a school decides to record pupils' biometric data.

The Data Protection Act 1998 can be viewed on the Office of Public Sector Information website [http://www.opsi.gov.uk/acts/acts1998/19980029.htm].

5.2   Pupil and parent consent

A question which is often asked is whether schools can legally collect biometric data without a pupil's or their parents' consent. There is nothing explicit in the Data Protection Act to require schools to seek the consent of parents before implementing a biometric technology system. The Data Protection Act 1998 provides that personal data shall not be processed unless one of the conditions of processing detailed in Schedule 2 of the Act [http://www.opsi.gov.uk/acts/acts1998/80029--n.htm#sch2] is met. Consent is one of these, but it is not required if any of the other conditions applies.

Regarding the age of a child, pupils are the data subjects of the personal data which is being collected and it is they who should in the first instance be informed about the use of their personal data. The Data Protection Act 1998 does not specify when a person is (or may be considered to be) too young to give consent. It is a matter of judgement that must be made on a case by case basis by the school as the data controller. Only where a pupil is judged to be unable to understand what is involved will his or her rights be exercisable by the parent or someone with parental responsibility for the pupil.

Whilst consent is not required for all processing of personal data, schools should normally involve pupils and parents in their decisions to use biometric technologies as is the case with other decisions made during the school life of children.

The ICO paper referred to in section 1 above contains a helpful discussion of consent issues.

5.3   Other legislation

While this document is aimed at providing guidance under the Data Protection Act 1998 in relation to the collection of biometric data, there are other legal considerations that apply to the collection of data more generally, such as the Human Rights Act 1998 and the common law of confidentiality. Schools may wish to consult more general guidance on these matters, in particular Chapter 2 and Appendix 1 of "Data processing and sharing: DfES guidance to the law" (listed in Further sources of information below).

As they judge appropriate schools may also wish to seek their own legal advice on these matters.

5.4   Security

Schools should recognise that security of personal data is of paramount importance and, for obvious reasons, a particular concern of parents. Under the Data Protection Act 1998, schools have a duty to ensure that all the personal data they hold is kept secure.

Becta have published functional and technical specifications for school infrastructure, available on Becta's Schools website:

- functional specification [http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_str_02&rid=11280]

- technical specification [http://schools.becta.org.uk/index.php?section=lv&&catcode=ss_lv_str_02&rid=11281].

The technical specification includes the detail of the ICT security measures schools should have in place, covering ICT security policies and procedures, physical security, data security, network security and internet and remote access security. Each area addresses the controls that need to be implemented in order to maintain an appropriate level of ICT security. Becta strongly recommends that schools consult both its functional and technical specifications for ICT infrastructure when considering introducing biometric technologies (as well as ICT more generally).

Section 6 below deals with the practical issues in more detail.

6   Practical steps schools should consider when introducing biometric technologies

Before introducing biometric technologies, schools should consider first with their governing body what system is most suitable and appropriate to their needs.

If having looked at all the facts a school decides to make use of biometric technologies for some of its administrative processes, and notwithstanding the legal position outlined in section 5 above, schools should recognise that some parents may have concerns about what is planned. In the light of such possible concerns, it is good practice for schools to be clear and open with all parents and pupils when introducing the technology. This could involve explaining what biometric technology will be used, what is involved, what data will be held and stored, why it is required, how it will be secured and how long it will be retained.

Schools should also reassure parents and pupils that they will not pass the data on to any third parties and explain how the personal data used will be kept safe. Finally they should reassure parents and pupils that all biometric data will be destroyed when the pupil leaves the school.

It may be that some parents and/or pupils will seek to opt out from using the biometric systems. In this case schools may want to build into their plans the option for some pupils to have an alternative means of accessing the same services (for example smartcards). This is in recognition that although schools are acting legally and that biometric data should be handled in the same way as other data (and subject to the Data Protection Act 1998), some parents may have concerns about such practice.

Further sources of information

- In addition to the paper mentioned in section 1 above, the ICO has also published technical guidance notes for schools in England, Wales and Northern Ireland on their responsibilities under the Data Protection Act regarding requests for access to pupils' information. [http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx].
- Data processing and sharing: DfES guidance to the law (information on data protection, the Human Rights Act and other related areas of law, largely in chapter 2 and Appendix 1) [http://www.teachernet.gov.uk/management/atoz/d/dataprocessing].
- Functional specification: institutional infrastructure, published by Becta, November 2005 [http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_str_02&rid=11280].

- Technical specification: institutional infrastructure, published by Becta, January 2007 [http://schools.becta.org.uk/index.php?section=lv&&catcode=ss_lv_str_02&rid=11281].