biometric technologies in schools

draft guidance for education authorities

GOOD GOVERNANCE

CONSULTATION

PROTECTING PERSONAL INFORMATION

smarter scotland
SCOTTISH GOVERNMENT

biometric technologies in schools

draft guidance for education authorities

The Scottish Government, Edinburgh 2008

ISBN: 978-07559-1815-7 (web only)

The Scottish Government
Victoria Quay
Edinburgh
EH6 6QQ

Produced for the Scottish Government by RR Donnelley B57556 9/08

Published by the Scottish Government, September, 2008

contents

Biometric Technologies in Schools

Guidance for Education Authorities

1. Introduction

1.1 This guidance is aimed primarily at education authorities, head teachers and their staff and parent councils. It is intended to provide education authorities, schools and parent councils with some of the basic information they need to know about biometric technology and its potential use within schools and some of the issues to be carefully considered before electing to put in place a biometric system. It also aims to provide some guidance as to good practice in implementing biometric systems within schools.

1.2 The decision to use biometric systems in schools is a decision for education authorities. This guidance is intended to assist education authorities in considering carefully the issues involved and, if they decide to opt for such a system, the good practice to be followed in implementing such systems. Key issues are whether the use of biometric data is proportionate (that is whether there is an identified need for this type of technology solution) and consideration of its potential impact for data subjects (see 8.1 below). The question of consent by users and their parents or guardians and the right to opt out without penalty, are also key issues.

1.3 The Information Commissioner has set out his view on the use of biometric technologies in schools and the statement can be accessed from the Information Commissioner's Office (ICO) website at www.ico.gov.uk, together with the accompanying press release. The guidance also draws considerably on the British Educational Communications and Technology Agency (BECTA) guidance on biometric technologies in schools, covering schools in England. We have also taken account of practice in some other jurisdictions.

1.4 Parents and carers may also find this guidance and the ICO's statement helpful in understanding what biometric technology is, its potential uses and what protections exist under legislation such as the Data Protection Act 1998.

1.5 It should be noted that only general guidance is provided in relation to the Data Protection Act 1998. As they judge appropriate, education authorities will wish to seek their own legal advice on these matters.

2. What is biometric technology?

2.1 Everyone has physical or behavioural characteristics that are unique to them and change little over time. Fingerprints are a well-known example and 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.

2.2 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 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 another).

2.3 There are two approaches to recording an individual's biometric characteristics. The first is to record a complete image of, for example, 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 most likely to be used in schools where biometric technology systems are put in place. A number of schools in Scotland have already put in place or are considering putting in place such systems. With such an approach the manufacturers of such systems state that the original cannot be reconstructed from the data. That is, it is not possible for example, to recreate a pupil's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

Biometric technology systems

3. School fingerprint or palm recognition systems

3.1 A number of the biometric systems that have been established or are being considered in Scottish Schools have typically been based on fingerprint or palm 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. These systems work in the following way.

Fingerprint recognition

3.2 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.

Palm recognition

3.3 The palm of the hand is placed above the sensor and a near infrared image captured. The vein pattern data is encrypted and the captured pattern data then encrypted and stored. Matching is with the template data.

4. Examples of the use of biometric technology in schools

4.1 Biometric technology has been promoted by manufacturers for a range of systems in schools. Some examples of such systems, showing the role that biometric technologies can play in them are described below. However, such systems do not have to be supported by biometric systems and other identification mechanisms (such as smartcards) can be used.

- 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 can be identified at the till by an automated fingerprint or palm recognition mechanism, with the cost of their lunch being deducted from the credit paid for by the parent. In some instances pupils can also add cash on themselves using machines based in the school;
- Automated system for recording attendance: Pupils register via an automated fingerprint or palm recognition mechanism at the school gate or entrance at the start and end of each day;
- School library automation: use of biometric technology to help manage lending from the school library. An automated fingerprint or palm recognition system identifies and records the pupil's name and the items they have borrowed or are returning.

4.2 Biometric technologies are said by suppliers to possess certain advantages over other automatic identification systems e.g. in relation to catering or borrowing books, pupils do not need to remember to bring anything with them to the canteen or school library, so nothing can be lost, such as a swipe card. On the other hand, biometric systems can be perceived as more intrusive than other systems. There is also the question of whether such systems are proportionate and appropriate for use in an educational environment (see 8.1 below).

Legislative context

5. The legal position and the Data Protection Act 1998

5.1 The introduction of biometric technology systems in schools is a matter for education authorities to consider.

Section 1 of the Education (Scotland) Act 1980 places a duty on every education authority to secure that there is made for their area adequate and efficient provision of school education and further education. Section 17(1) places a further duty to provide for their area sufficient accommodation in public schools and other educational establishments under their management to enable them to perform their functions. The education authority may, for the purposes of fulfilling this duty, provide, alter, improve, enlarge, equip and maintain schools and other educational establishments outwith as well as within their area.

Under section 2 of the Standards in Scotland's Schools etc. Act 2000 where school education is provided to a child or young person by or by virtue of arrangements made or entered into by an education authority, it shall be the duty of the education authority to secure that the education is directed to the development of the personality, talents and mental and physical abilities of the child to their fullest potential. Section 2(2) provides that in carrying out this duty the education authority shall have due regard, so far as reasonably practicable, to the views (if there is a wish to express them) of the child or young person in decisions that significantly affect that child or young person taking into account their age and maturity.

5.2 If an education authority decides to introduce and use such systems, it 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.

6. The Data Protection Act 1998

6.1 Education authorities 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 (hereinafter referred to as "the Act").

6.2 Education authorities are "data controllers" in terms of the Act since they determine the purpose(s) for which, and the manner in which, any personal data are processed. Data which relate to individual pupils who can be identified from that data (or from that data and other information which the education authority holds) will qualify as personal data in terms of the Act. The pupils to whom the information relates are the data subjects. When personal data relating to and identifying pupils are obtained, education authorities must ensure that the pupils and/or the parents/guardians as appropriate (see section 9 below) are provided with a *Fair Processing Notice* which will contain information as to:

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

6.3 In addition, education authorities must comply with the following Data Protection principles which state that data must be:

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

6.4 As far as the Act is concerned, biometric data must be handled in the same way as any other personal data and the same principles as above apply when an education authority decides to record pupils' biometric data.

7. Other legislation

7.1 While this document primarily provides guidance in respect to the Act 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 duty of confidentiality. As they judge appropriate, education authorities will wish to seek their own legal advice on these matters.

Consideration of the introduction of biometric systems

8. Issues to be carefully considered before electing to put in place a biometric system

8.1 An important question to be addressed when considering the installation of a biometric system is whether there is an identified need for this type of technology and its potential impact for data subjects, by considering factors such as:

- the school environment – does the nature of the school or college environment require high levels of security?
- existing systems – is the adequacy, efficiency or reliability of existing systems in doubt, such that a new solution is required?
- has there been an examination of a number of types of system solutions, both biometric and non-biometric that are available?
- what are the evidenced benefits of a biometric system over other options?
- could an alternative such as a smartcard be a less intrusive solution and provide the same outcome?
- has a privacy impact assessment been carried out (see 8.4 below)?
- can the biometric system provide transparency of operation, accuracy of data and appropriate security, to ensure the principles and requirements of the Act are met?
- is the biometrics application a self-contained system, whose templates cannot readily be used by computers running other fingerprint recognition applications?
- can an effective and user friendly system be put in place for pupils who wish to opt out of any biometric system?
- is the authority confident that pupils who are unable to provide biometric data, because of a disability for example, will not be discriminated against by being required to operate a different system?

8.2 Education authorities are reminded that it is not necessary to introduce biometric systems to meet the duty set out in the Schools (Health Promotion And Nutrition) Scotland Act 2007, to take reasonable steps to ensure that those in receipt of free school meals cannot be identified as such by anyone other than an authorised person. There is a variety of ways in which this can be achieved, which do not require a biometric type solution, e.g. smartcards. Given the necessity to cater for those wishing to opt out (section 9.6 below) and to take account of those with disabilities (section 15 below), a biometrics based system probably cannot be justified *purely* as a response to this requirement of the Act.

8.3 It is essential that the views of parents and pupils on the introduction of such technology should be sought by education authorities at this early stage.

8.4 A Privacy Impact Assessment is a risk management technique. The Information Commissioner's Office notes that:

"Projects that involve personal information or intrusive technologies inevitably give rise to privacy concerns. Where the success of a project depends on people accepting, adopting and using a new system, process or programme, privacy concerns can be a significant risk factor that threatens the return on the organisation's investment. In order to address this risk, it is advisable to use a risk management technique commonly referred to as a Privacy Impact Assessment (PIA)."

A Privacy Impact Assessment Handbook is available online at the website of the Information Commissioner's Office www.ico.gov.uk or by following this link ICO – Privacy Impact Assessment.

Implementation of biometric systems

9. Pupil and parent consent

9.1 There is nothing explicit in the Act to require education authorities to seek the consent of all parents before implementing a biometric technology system. The Act provides that personal data must be processed fairly and lawfully and, in particular, shall not be processed unless one of the conditions of processing detailed in Schedule 2 of the Act is met. Consent is one of these, but it is not required if any of the other conditions apply (see Appendix 1).

9.2 The Information Commissioner indicates, in the statement referred to earlier, that for the purposes of the Act, the pupils themselves are "data subjects". That is, it is they who should in the first instance be informed and consulted about the use of their personal data. However, the Commissioner goes on to say:

"Deciding when children are mature enough to decide how their personal information should be used is difficult. On the one hand, as children mature they are entitled to an increasing measure of autonomy. On the other hand, while children might understand a simple explanation of why their fingerprints are being taken, they may well not appreciate the potential wider implications."

As noted previously there is nothing explicit in the Act to require education authorities to seek consent from all parents before implementing a biometric system. However, the Information Commissioner states that:

"…unless schools can be certain that all children fully understand the implications of, for example, giving their fingerprints, then they must fully involve parents in order to ensure that the information is obtained fairly. Parents play a central role in their children's education, in terms of support and guidance, and also in terms of legal liability, for example, in case of truancy. They, therefore, rightly expect to be informed and consulted when biometric systems are introduced in their child's school. Suspicions are only likely to be increased when new and possibly controversial technology is introduced without a comprehensive effort to address people's fears and concerns."

9.3 In addition, the Standards in Scotland's Schools etc. Act 2000 requires an education authority to have due regard to the views of the children or young persons in decisions that significantly affect them, taking account of the child or young person's age and maturity. The Act also requires that education authorities, in their annual statement of improvement objectives, include an account of the ways the authority will seek to involve parents in promoting the education of their children. The Scottish Schools (Parental Involvement) Act 2006 describes the duty of an education authority to promote the involvement of parents in the education provided by the school.

9.4 **Before deciding to install a biometric system, the Scottish Government would expect that a properly documented privacy impact assessment is carried out (see paragraph 8.4). The Scottish Government would also expect that any education authority considering introducing biometric technology into one or more schools will inform and consult both pupils and parents. It is important for education authorities to be clear and open with all parents and pupils when introducing the technology. This will involve providing clear and unambiguous information for children and parents to ensure that they are fully aware of what is proposed and why, what information will be kept and how and for how long and how it will be secured. Information should also be given about how to opt out and consent issues. That information could also set out the rights to privacy that children have under Article 8 of the European Convention on Human Rights and Article 16 of the United Nations Convention on the Rights of the Child.**

9.5 Education authorities should also be able to reassure parents and pupils that they will not pass the data on to any third parties without the consent of the data subject, (except where one of the other conditions specified in schedule 2 of the Act (see Appendix 1) can be met) and explain how the personal data used will be kept safe. They should also have clear retention policies that allow them, for example, to reassure parents and pupils that all biometric data will be destroyed when the pupil leaves the school.

9.6 Education authorities should respect the wishes of those pupils and parents who object to initiatives involving biometric technologies. Other systems such as smart cards, where a card can work just as well as a fingerprint, are relevant here so that those who wish to "opt out" can be given another means of accessing the same services. Parents and pupils should be made aware of the option to opt out, and also what alternatives will be provided. Education authorities should reassure parents that, for example, the Young Scot card is not capable of holding biometric data and that these data will not be held on educational authority pupil records.

10. Security

10.1 Education authorities should recognise that security of personal data is of paramount importance and, for obvious reasons, a particular concern of parents. Under the Act, education authorities have a duty to ensure that all the personal data they hold are kept secure from unauthorised processing and accidental loss, destruction or damage. This would reflect the seventh principle in Schedule 1, Part 1 of the Act:

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

10.2 BECTA, which has a UK wide remit, has published functional and technical specifications for school infrastructure, available on its website http://industry.becta.org.uk. 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.

10.3 Education authorities implementing a biometric system should review existing levels of security and documentation in respect to this and ensure these are adequate for the introduction of any biometric system.

11. Accuracy

11.1 Schedule 1, Part 1(4) of the Act states that "Personal data shall be accurate and, where necessary, kept up to date". Therefore authorities must be confident that any biometric system will accurately identify the persons whose data are being processed by the system and that if changes in physical or psychological characteristics result in a template becoming outdated, a procedure will be in place to ensure that the template and hence the data, is kept up to date.

12. Access and use of data

12.1 There should be clear procedures and rules restricting access to any data or logs to authorised persons only who require such access in order to implement the system. Such procedures should specify why, when and how such access will be permitted. Data should not be passed on to any third parties, excepting where allowed for in the Act (see paragraph 9.5 and Appendix 1).

12.2 Biometrics applications should be self-contained systems, whose templates cannot readily be used by computers running other fingerprint recognition applications.

12.3 Pupils' biometric data should not be used for any purpose not directly related to that for which it was collected. This would reflect the second principle in Schedule 1, Part 1 of the Act:

"Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes."

12.4 It should be noted that section 10 of the Act, provides that a data subject can write to give notice to a data controller to cease processing personal data (except where one of the other conditions specified in paragraphs 1 to 4 of Schedule 2 of the Act (see Appendix 1) can be met), if the processing is causing or is likely to cause substantial damage or distress to the data subject or another person and that damage or distress would be unwarranted.

13. Retention

13.1 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 for keeping biometric data.

13.2 Personal data should not be kept for longer than it is needed for its specific purpose. It is envisaged that as soon as a pupil permanently leaves the school, his/her biometric data would be immediately deleted. This would reflect the fifth principle in Schedule 1, Part 1 of the Act:

"Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes."

14. Data protection policy

14.1 The education authority should update its existing data protection policy to take account of the introduction of a biometric system for pupils.

15. Taking account of the needs of pupils with disabilities

15.1 Education authorities also need to consider how they will ensure that pupils, who are unable to provide biometric data, because of a disability for example, are not discriminated against by being required to operate a different system.

16. Critical risk management

16.1 The education authority should ensure that adequate back up systems and plans are in place to cover any breakdown of the system.

17. Responses to consultation

17.1 Comments are invited on the draft guidance by **4 December**. Responses should be sent together with a completed Respondent Information Form to:

Russell.Cockburn@scotland.gsi.gov.uk

Or by post to:

Consultation on Biometric Technologies in Schools –
Draft Guidance for Education Authorities (CRES – CON 1065)
Support for Learning Division
Schools Directorate
Scottish Government
Victoria Quay
Edinburgh EH6 6QQ

17.2 If you have any questions about this consultation document please contact Russell Cockburn on 0131 244 4482.

APPENDIX 1

DATA PROTECTION ACT 1998

SCHEDULE 2
Section 4(3)

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

1 The data subject has given his consent to the processing.

2 The processing is necessary:

(a) for the performance of a contract to which the data subject is a party, or

(b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3 The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4 The processing is necessary in order to protect the vital interests of the data subject.

5 The processing is necessary:

(a) for the administration of justice,

(aa) for the exercise of any functions of either House of Parliament,

(b) for the exercise of any functions conferred on any person by or under any enactment,

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6 (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the 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 rights and freedoms or legitimate interests of the data subject.

(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

ISBN: 978-0-7559-1815-7 (web only)

RR Donnelley B57556 09/08

w w w . s c o t l a n d . g o v . u k