Biometric Technologies in Schools

Draft Guidance for Education Authorities: Consultation Analysis Report

February 2009

The Scottish Government

Introduction

1. This document reports on the consultation exercise held between 9 September 2008 and 4 December 2008 on the document entitled '**biometric technologies in schools: draft guidance for education authorities'** (the draft guidance). The draft guidance can be found on the Scottish Government's website.

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 The draft guidance, aimed primarily at education authorities, head teachers and their staff and parent councils, is intended to provide some of the basic information about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

3. This report also sets out what impact the consultation findings will have on the draft guidance.

4. Along with the responses to the consultation, the Scottish Government will be considering the opinions of the Principles Expert Group which was established to help public bodies protect individuals' privacy and to help increase public confidence in IT-enabled public services. The group will advise the Scottish Government on high level principles on identity assurance and privacy for public services which are enabled by IT. Members of this group have provided advice on the draft guidance. As part of the two objectives, i.e. developing draft principles and giving advice on the Biometrics Guidance, the group is considering appropriate uses of biometric and other technologies in relation to public services in Scotland.

5. As part of that, the members of this group have been considering the practical implications of the principles in relation to existing and new systems, covering professional and practioner roles, staff procedures and protocols, monitoring and audit and governance.

6. We received a wide range of responses to this consultation. While not all of these are mentioned explicitly in this report, we have carefully considered all responses. The sample views in the report have been included to give a flavour of the opinions expressed.

Background

7. Ministers decided that guidance was needed to provide education authorities, schools and parent councils with information about biometric technology, its potential use within schools and the issues to be considered before electing to use a biometric system after it was brought to the attention of the Scottish Government that systems were already in use in some schools.

8. When Fiona Hyslop, Cabinet Secretary for Education and Lifelong Learning launched the draft guidance on 9 September 2008, she said:

> "We know that some schools are already using biometric technology to provide access to school meals and other functions. Security and privacy issues are a very serious concern in relation to the use of biometrics in schools and this must be fully addressed. That is why we are issuing this draft guidance today. It will be an important tool to assist schools, with the involvement of parents and pupils, in ensuring this.
>
> The draft guidance will be consulted upon over the next three months and then issued in a finalised form taking account of the responses received and advice from the expert group.
>
> This Government is committed to putting civil liberties at the heart of public services policy. It is important that schools pupils are made aware of the importance of their personal information in relation to any biometric service for school meals or library access. When using IT, we need to ensure the mechanisms involved are designed and delivered in such a way that individual privacy is respected. That is why we are developing principles to guide public bodies when designing or developing public service systems and why consultation on how we manage biometric technology in schools is very important."

9. We received 24 responses to the consultation from a range of consultees including 14 out of the 32 Scottish local authorities. All published consultation responses can be viewed on the Scottish Government's website.

10. The responses to the consultation and the advice of the Principles Expert Group generated a variety of views which have been essential in informing potential amendments to the draft guidance. We would like to thank all those who took part in the consultation process for their views.

Consultation Report

Part 1: Comments on the Draft Guidance

General feedback on the draft guidance document

Sample responses:

- "The draft guidance provided is full and comprehensive in its assessment of the issues and the advice it provides within each section". (East Ayrshire Council)

- "On the whole the document is neutral and objective and leaves the final decision to the local authority and/or school. It presents clear examples of for and against." (The Moray Council)

- "Overall the draft guidance is a good and balanced document that addresses well the areas that education authorities should consider when deciding whether to make use of biometric technology". (No2ID)

11. Comments on the general content of the draft guidance were typically supportive.

12. Eleven local authorities responded to the consultation with their own comments on the draft guidance (as opposed to comments submitted to them on behalf of schools, parent councils and individuals from within their authority area). Seven offered general feedback on the document as a whole, describing it as 'clear', 'full and comprehensive', 'unbiased', 'balanced' and 'helpful'.

13. Another three local authorities responded to the consultation by offering an analysis of responses to the guidance which had been submitted to them by individuals, schools and other stakeholders from within their authority area. Two of these analyses (those from City of Edinburgh Council and Perth and Kinross Council) have been published on the Scottish Government's website along with all other responses to the consultation. One authority requested that its submission not be made publicly available.

14. Of the other responses received to the consultation, there are five which comment directly on the content of the draft guidance while a further five offer more general comments on the potential use of biometric technologies.

15. Members of the Expert Group also commented on the draft guidance document and made submissions individually. These submissions, though not published on the Scottish Government website, will also contribute towards any revision of the draft guidance.

Biometric Technologies in Schools
Guidance for Education Authorities

Section 1. Introduction

Sample responses:

- "The guidance neatly directs authorities to consider whether biometrics is the right solution to the problem trying to be solved." (Aberdeenshire Council)
- "It would be useful if the introduction clearly specified the potential uses of biometric technologies in schools." (Dundee City Council)
- "Section 1.2 States clearly that the use of biometric systems in schools is a decision for education authorities to make. It informs authorities of good practice to be followed in implementing such systems. It asks if there is an identified need for such technologies and lists as key issues, the question of consent by users and their parents including the right to opt out without penalties" (Wester Cleddens Primary School, School Board)

16. The Introduction of the draft guidance explains who it is primarily aimed at, where the decisions to implement a biometric system rest and what other guidance is available. It also mentions some of the issues which are to be discussed within the document such as the question of consent and the right to opt out.

17. Eight responses made specific comments on the issues outlined in the introduction of the draft guidance. One respondent was concerned that the use of the term "good practice" in paragraph 1.1 indicated an assumption that these technologies would be used in schools. As already noted, it is the case that biometric technologies are being used in Scottish schools and that is why we have produced the guidance. Conversely, another respondent commented that the recognition that "some Scottish schools – like schools around the world – will be considering using biometric systems" as "welcome".

18. There was a suggestion in one response that a list of potential uses of biometric technologies within schools should be included in the introduction of the guidance. Examples of the use of biometric technologies in schools are given in section 4.1 on page 4 of the draft guidance. It is not an exhaustive list and further uses may emerge in time.

19. Another response indicated that it was helpful that the guidance emphasised early on that any decision on the implementation of biometric systems in schools was a decision for the education authority. Other responses, however, raised concerns about the fact that this decision is one for education authorities to make. One respondent suggested that "it would be preferable if the good practice contained within [the draft guidance] were to be placed on a statutory footing rather than being left at the discretion of education authorities." Another considered that "there is compelling need to consider the matter within the

Scottish Parliament, particularly to consider wider issues of civil liberties and to consider giving national effect to the "opt out" principal".

20. These concerns, while certainly pertinent to any debate surrounding the use of biometric systems, focus on legislation rather than how existing legislation and good practice is expressed in guidance.

Section 2. What is Biometric technology?

Sample responses:

- "While paragraph 2.1 identifies some measures that can be used, it must also be recognised, that other measures, such as DNA or body odour recognition may also be used." (EIS)

- "The guidance is clear and concise in its description of the technology and the type of systems that exist. During the description of the technology, the guidance does well to take the opportunity to raise the question of proportionality once again and directs authorities to ask themselves the question on whether this is the right use of technology to solve an education establishment problem." (Aberdeenshire Council)

21. This section of the draft guidance covers what is meant by biometric technology; the administration of these technologies; approaches to recording biometric information and the reverse engineering of images from stored, encrypted, numeric data.

22. A number of the comments on this section of the guidance were concerned with the last of these issues, pointing out that there is "debate by experts as to whether, in fact, this [the reverse engineering of images] might be possible in the future, and perhaps this view needs to be included in the document with a reassurance that a watching brief on emerging developments regarding fingerprint and palm recognition would be maintained, and by whom."

23. Other respondents expressed similar concerns about the wording of paragraph 2.3 of the draft guidance. One respondent pointed out that "Allegedly foolproof encryption strategies may prove to be anything but, and we would welcome clarification in the guidelines as to whether the numberstrings and/or algorithms into which a biometric is converted could ever itself be used to identify an individual independently of the system-in-use within a given school."

24. This respondent also suggested questions that should be considered before electing to use biometric technologies within a school such as: "What would happen if the technology broke down?", "Will data be backed up in another place – which, if so, suggests that data is electronically transferrable – or will pupils simply be required/asked to re-register if the first finger or palmprint they gave becomes unusable?" "Will the numberstrings into which the biometric identifiers are converted ever be stored on – easily mislaid – CDs or flashdrives?" Also, "Will any local authority ever have remote access to the computers on which encrypted biometric data is stored?"

25. Another response asserted that “contrary to vendors’ claims, it is possible to reconstruct images from stored templates” and that there is “widespread published literature on methods for reconstructing images from templates.” Furthermore, it claimed that “it is not actually necessary to reconstruct original images for the privacy of subjects to be invaded.” and that “Someone attempting to match a print to a child could identify the child by running the print through the enrolment algorithm to generate a template. Comparing the generated template with those stored in the database would yield a match with the person to whom the print belonged.”

26. The possibility of the type of situation described above occurring, while impossible to eliminate entirely, can be diminished. The draft guidance states in paragraph 8.1 that one of the considerations to be made before electing to install a biometric system is whether a Privacy Impact Assessment (PIA) has been conducted. In conducting a PIA, aspects of any project under consideration would include design issues and the identification of ways in which negative impacts on privacy can be avoided.

27. The Information Commissioner’s Office (ICO) state in their response to the consultation that “In considering the introduction of biometric systems, the ICO would encourage the use of the check-list provided within the consultation paper to assist in justifying the decision. Moreover, the ICO is particularly pleased to see the emphasis placed on carrying out a Privacy Impact Assessment (PIA) prior to the introduction of a biometric system. PIAs are an excellent tool in identifying potential privacy costs and benefits and formulating strategies to address problems at the outset of policy development as it is much more costly to try to address negative privacy impact after implementation. **The ICO would be happy to work with any education authority considering introducing biometric technologies in its schools.**”

28. On the issue of the reconstructing of images from encrypted numeric data, the ICO state that “The obvious benefit of a derived numeric is its resistance to reverse engineering for nefarious use” and that “this system is less intrusive and is more secure”. They make the recommendation that “**converting data into a numerical value is the only system used**.”

29. A response which was received from a software company claims that if the unencryption of an algorithm were possible, “the unencrypted algorithm can match one of many thousands of other algorithms. An algorithm is not unique, and is only of use when compared against the same finger being used in another application.” In the same response the point is made that “Should anyone wish to capture biometric data from an individual they need only to procure a glass that the individual has held, and they have a permanent record of someone’s biometric.”

30. This, of course, is a statement of the approach of this one particular company and does not negate the importance of attention to the seventh data protection principal as also indicated in paragraph 73.

31. There is clearly a concern about the statement in paragraph 2.3 of the draft guidance that biometric information "cannot be reconstructed from the data". We will reconsider the wording of 2.3 when redrafting the guidance.

Biometric technology systems

Section 3. School fingerprint or palm recognition systems

Sample responses

- "Hygiene concerns arise from having every child in a class/school touching the same piece of plastic or glass. This is of particular concern when children use biometric payment systems and touch the equipment immediately prior to eating." (No2ID)

- "What are we saying to our young people when we are scanning their palms, fingerprints and not trusting them to handle money??" (Jackie Marshall)

- "The practice of fingerprinting is inevitably linked with criminal activity and can therefore be seen as stigmatising those having their fingerprints taken." (Information Commissioner's Office)

32. Section 3 of the draft guidance gives a detailed outline of how biometric systems – which measure biometric data from fingerprints or palm vein patterns – generate numerical values which are stored in a database and then matched against a number generated on each repeated use to identify pupils.

33. There were many comments from respondents concerning the use of fingerprint and palm vein pattern recognition systems and there was also substantial coverage of this issue in the submissions received from the members of the Principles Expert Group. These comments addressed issues such as "what is perceived by parents to be the conditioning of children to accept being fingerprinted as a routine part of life"; hygiene concerns that "arise from having every child in a class/school touching the same piece of glass."; that "There is something quite sinister about palm scanning and finger print scanning"; and that "fingerprinting - has, an image traditionally and still associated with policing and criminal justice."

34. We are not convinced that issues of hygiene need to be covered in the guidance as similar issues affect the use of systems which do not use biometric technology. Most of the comments on these technologies are statements of opinion on the suitability of any such systems for use within the school environment.

35. The emphasis on the proportionality and suitability of any biometric system is consistent throughout the draft guidance, as respondents to the consultation indicated:

- “During the description of the technology, the guidance does well to take the opportunity to raise the question of proportionality once again and directs authorities to ask themselves the questions on whether this is the right use of technology to solve an education establishment problem“ (Aberdeenshire Council)

- “Para 1.2 of the guidelines raises the question of whether or not biometrics are a proportionate response to an identified problem within a school, and whether or not there may be other solutions.” (The University of Strathclyde)

36. This is emphasised in paragraph 8.1 in particular, where a checklist of considerations is presented along with the advice that “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”. Education authorities should consider suitability during their deliberations. Ultimately, however, these decisions are for education authorities to make.

37. In light of the number of responses received to the consultation questioning the proportionality of implementing biometric systems in schools, we will consider whether it is necessary to make this clearer still in the revised guidance.

38. Further discussion around the opinions expressed in the consultation on aspects of fingerprint and palm vein pattern recognition systems, along with discussion of other comments received which don’t directly engage with the content or wording of the guidance, are in Part 2 of this report.

Section 4. Examples of the use of biometric technology in schools

Sample responses:

- “None of the examples set out in section 4.1 appear to be compelling reasons to adopt biometric technologies.” (EIS)

- “Para 4.2 of the draft guidelines notes that “biometric systems can be perceived as more intrusive than other systems”. Insofar as they make use of parts of the body as personal identifiers, in a way that other access and registration systems do not, it is easy to see why civil libertarians have claimed them to be intrusive.” (University of Strathclyde)

39. Section 4 of the guidance gives a short list of examples of a range of systems for which the use of biometric technology is recommended by the manufacturers. It explains that these systems do not need to be supported by biometric technology and again draws attention to the issue of proportionality.

40. As mentioned in the analysis of the introduction, this list has been included to demonstrate some of the potential ways in which biometric technology can be deployed and is not to intended to either encourage or discourage its use.

41. One respondent, however, commented that although paragraph 4.1 highlights that the systems mentioned in the bullet points do not necessarily require support from a biometric system, the only alternative suggested is a smartcard system.

42. The guidance provides advice on issues that should be considered in relation to their deliberations regarding biometric system in schools. It is not considered appropriate to include a comparative analysis of the benefits of various other systems. These are issues to be explored by those most intimately aware of the requirements of any potential system and who would ultimately be responsible for its implementation. In these circumstances, that would be an education authority. It is not the intention for any section of this guidance to either promote or discourage the use of biometric systems.

43. In light of issues referred to in paragraph 18 as well as those comments received on section 4, we will consider the wording of section 4.1 in redrafting the guidance to ensure that the purpose of including these examples is unambiguous and to ensure that they are not construed as a full set of the circumstances in which biometric technologies may be used.

Legislative Context

Section 5. The legal position and the Data Protection Act 1998

Sample Comments:

- "Inverclyde Council considers that the document is very clear and that the legislative context has been clearly identified." (Inverclyde Council)

- "This section is very useful as a guide to the various requirements of the legislation to be taken account of when considering the possible introduction of biometric technology." (Renfrewshire Council)

- "The inclusion of guidance on the age by which children are deemed to be of sufficient maturity to comprehend the key principles within the Data Protection Act, or a test other than age, would be helpful." (Aberdeenshire Council)

- "As the draft guidance states, the seventh data protection principle requires that personal information is kept secure against unauthorised or unlawful processing, including accidental damage or loss. The recent high profile data losses have done much to undermine the confidence in data controllers to process securely our personal information. It is imperative therefore that all staff be given appropriate guidance and training in any new system in particular but also in their responsibilities in terms of data protection more generally." (Information Commissioner's Office)

44. Section 5 of the draft guidance discusses legislation pertinent to considerations when contemplating the introduction of a biometric system within a school. Section 6 explains some of the considerations with special regard to the Data

Protection Act 1998. Section 7 considers the implications of other relevant legislation. Responses generally commented on these sections of the guidance together.

45. These sections were commented on by several respondents. Many of these comments were supportive, describing this section as "a useful set of issues to be considered by local authorities, prior to electing to install a biometric system" and that the draft guidance is "helpful in addressing the legislative implications and the practical considerations of the introduction of such a system".

Section 6. The Data Protection Act 1998

46. One respondent pointed out that this section "usefully re-emphasises that any decision to be made on the introduction of biometric technology is a matter for education authorities to consider" while another respondent expressed support for the view of the ICO "that the first, second, fifth and seventh principles of the Data Protection Act 1998 are most relevant to the issue of biometric systems for children and young people."

47. The ICO response states that although it is a "common misconception that all processing of personal information must take place on the basis of consent this is not the case. However, fair processing requires that children and parents are fully informed about what is being proposed and what this will mean in practical terms for the child." The ICO also say that "as the draft guidance points out, where an opt-out is possible there must be a pre-conceived strategy for dealing with those children who, for whatever reason, choose not to use the system".

48. It should be stressed that education authorities should seek their own legal advice on the need for consent. We agree with the ICO in that good practice would require that children and parents are fully informed.

49. The ICO also comment on the draft guidance's mention of the seventh data protection principle of the Data Protection Act 1998. This "requires that personal information is kept secure against unauthorised or unlawful processing, including accidental damage or loss." Accordance with this principal may require "that all staff be given appropriate guidance and training in any new system in particular but also in their responsibilities in terms of the data protection more generally."

50. The response from the University of Strathclyde points out that "The guidelines don't directly or clearly address the issue of whether informed consent MUST be given to schools, but in allowing for opt-out systems for those who by definition have not consented, it implies that consent must be given." It goes on to say the "guidelines could usefully be more explicit about this and specify any circumstances when the introduction of biometric identification systems – indeed any surveillance systems – in school might, if ever, be vetoed or reversed."

51. We will consider whether it is possible to clarify this in the revised guidance in light of the advice we received from the Principles Expert Group.

52. Another respondent asked specific questions on the content and wording of this section of the guidance. In the last bullet point of paragraph 6.2, the respondent asked "Who decides which third parties are granted access to the information, and are there any controls on which third parties the third parties grant access to?"

53. Controls on who can process personal data and under what circumstances are set out in the Data Protection Act. As 6.4 of the draft guidance states, "biometric data must be handled in the same way as any other personal data"

54. The circumstances under which personal data may be shared with a third party without the consent of the "data subject" are laid out in Schedule 2 of the Data Protection Act 1998. This is included in the draft guidance at Appendix A. In all other circumstances, the consent of the "data subject" is required for any third party to be granted access. Any third party who is granted access to that information would then be subject to the same restrictions that the Data Protection Act places on that information and could not share it with another party unless consent of the "data subject" was granted.

55. We will consider whether this section of the guidance requires more detail on the duties of the Data Protection Act in the revised guidance.

Section 7. Other Legislation

56. One respondent commented that the "document provides guidance in respect to the Data Protection Act 1998 but also mentions that there are other legal considerations that apply to the collection of data e.g. the Human Rights Act 1998 and the common law of confidentiality. The suggestion is that local authorities will wish to seek their own legal advice on these matters. It might have been helpful if the consultation document went into this aspect of the law in more detail."

57. We will determine whether more consideration needs to be given in respect of other legislation when the guidance is redrafted.

Consideration of the introduction of biometric systems

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

Sample Responses:

- "The checklist contained in this section is very useful in clarifying if a biometric system is required at all." (East Renfrewshire Council)

- The factors for consideration specified in 8.1 are extremely useful and are likely to assist in any decision-making process. (Dundee City Council)

58. Section 8 of the draft guidance contains a list of issues which should be considered before an authority makes the decision to implement a biometric system. It makes clear that the Schools (Health Promotion and Nutrition) (Scotland) Act 2007 does not require the implementation of a biometric system and that views of parents and children ought to be sought early in deliberations. It also contains a brief explanation of the PIA process.

59. The list of issues to be considered before electing to put a biometric system in place was welcomed in several responses. Other responses suggested amendments to the bullet points in section 8.1.

60. One local authority suggested that this "could be further strengthened by the inclusion of questions which direct the authority to look in more detail at the problems and issues that have caused it to think about biometrics. It may be that a more fundamental problem exists in terms of the structure or organisation that needs to be addressed before biometric needs to be considered. In effect, is biometrics the right solution to the right problem?"

61. A criticism which arose in more than one response was that where the draft guidance states that there "is a variety of ways in which this can be achieved, which do not require a biometric type solution, e.g. smartcards", that smartcards are the only alternative solution which is mentioned. One respondent suggested that it "would be helpful if the final guidance document was broadened out to contain an assessment of the perceived advantages and disadvantages of card based systems. It would also be helpful if further alternative systems were referred to, again with an assessment of their strengths and weaknesses. "

62. The primary aim of the guidance, as stated in the introduction to the draft document, is 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". The focus of the document is provision of information regarding biometric systems. It is for education authorities to make the final decision about whether this is the type of system which most adequately fits the requirements of an individual school as they will have the most intimate knowledge regarding the requirements of any potential system. Given that education authorities will be best placed to know these requirements, it is right that they conduct their own research when deciding which system to implement.

63. We will consider whether further alternative systems should be mentioned in this section of a redrafted guidance document. However, as stated in paragraph 42, it is not appropriate for an assessment of the comparative strengths and weaknesses of these alternatives to be included in a guidance document on biometric technologies.

Implementation of biometric systems
Section 9. Pupil and parent consent

Sample responses:

- "We believe the question of opt out recognises that a significant number of parents and pupils will have sufficient reservations about biometric technologies to be resistant to their use. However it is not clear whether Councils will be required to allow "opt out" (EIS)

- "This section contains very sensible advice regarding the need for full consultation with both parents and pupils." (Dundee City Council)

- "The guidance is clear in the information it provides on the need and desirability of consulting pupils and parents on this issue" (Aberdeenshire Council)

64. Section 9 covers issues concerning consent for consideration when implementing a biometric system. It clarifies the legal aspects of obtaining consent with special regard to the Data Protection Act 1998 and the Standards in Scotland's Schools etc. Act 2000, explains the position of the ICO and includes a passage in bold text setting out what we consider to be good practice.

65. As stated in paragraph 49, concerns were raised in the University of Strathclyde response about whether "informed consent MUST be given to schools". We would recommend that education authorities seek their own legal advice on this issue. As stated previously, we consider that good practice requires that parents and pupils are kept informed and involved when contemplating the use of a biometric system in a school.

66. Authorities should also consider the importance of allowing for an opt-out system for those who do not consent as, other than under specific circumstances set out in the Data Protection Act, a child could not be made to use a biometric system against his or her will. This, however, does not imply that the consent of all children and parents must be obtained before a biometric system is implemented, but that we expect an authority which is considering the implementation of a biometric system will inform and consult both pupils and parents. If it is apparent from such a consultation that a significant number of parents and pupils do not want a biometric system in their school, the authority may wish to reconsider its use.

67. We will consider whether this point requires clarification in the revised guidance.

Section 10. Security

Sample responses:

- "The advice in this section is particularly welcomed, especially in the light of several recent press reports of incidents concerning loss of personal data." (Dundee City Council)

- "if school databases are compromised, there is potential for adverse effects on children's future lives." (No2ID)

- "Recent losses of data and subsequent fall-out must raise concerns re the security of any system." (SSTA)

- "Children and parents must feel confident that their personal information will be secure." (Information Commissioner's Office)

68. Section 10 deals with issues related to keeping biometric data secure. It emphasises the duties of data controllers under the Data Protection Act, draws attention to the functional and technical specifications published by the British Educational Communications and Technology Agency (Becta) and recommends a review of existing security levels when contemplating the implementation of a biometric system.

69. The ICO emphasises the importance of data security in their response pointing out that, as the guidance states, "the seventh data protection principal requires that personal information is kept secure against unauthorised or unlawful processing, including accidental damage or loss." It recommends that "a record is kept of access in terms of who is accessing the system, when, how and why. The ICO further recommends that the database is kept local to the school operating system."

70. Concerns about the security of the data were raised in several of the responses with more than one respondent citing "recent press reports of incidents concerning the loss of personal data." This was also raised in the comments provided on section 2 which referred to "easily mislaid" CDs and flashdrives.

71. One comment included in the Perth and Kinross Council response suggested that the draft guidance "appears to present possibilities rather than actualities: insufficient identification and explanation of safeguards provided." However, in response to the question: "Does the guidance effectively explain the Data Protection implication of biometric technologies?" ten contributors to the Perth and Kinross response answered "Yes" with only two contributors saying "No".

72. Conversely, the response to the consultation from a software company which manufactures biometric systems states that "[we are] dependent on success, and endeavour to ensure that we maintain our reputation. A breach of security, or severe failure of the technology would perhaps fatally disrupt our business. We are constantly seeking to introduce new features and technology to add to the security of our implementations." They also offered an assurance that

“Back ups are encrypted and can only be accessed when used with secure servers that have encrypted licence keys.”

73. The above is, of course, is a statement of the approach of this one particular company and does not negate the importance of attention to the seventh data protection principle. This principle is emphasised within this section of the draft guidance because it has particular relevance when considering issues of data security. The intention is to emphasise the importance of ensuring that security measures are adequate for the introduction of a biometric system. We will consider whether this requires more explicit expression in the revised guidance.

Section 11. Accuracy

Sample responses:

- “Biometric enrolment tests performed on behalf of the Home Office encountered verification failure rates of 1 in 5 for fingerprint recognition. The Shirley McKie case should also give pause for thought.” (No2ID)

- “special attention has to be given where the biometric information changes with age.” (Information Commissioner’s Office)

- “We accept that biometric technology would be a huge step towards ensuring 100% accuracy in registering pupils but are not aware of any problem with the current system which we believe to be very accurate” (SSTA)

74. Section 11 seeks to highlight the importance of accuracy when recording biometric data to satisfy the requirements of the Data Protection Act. Within this section of the guidance, the term ‘accuracy’ is intended to refer to the veracity of the data and not to the level of detail. Where the Data Protection Act states in Schedule 1, Part 1(4) that “Personal data shall be accurate and, where necessary, kept up to date” it refers to necessity of ensuring that information recorded must not be false. It does not intend any inference regarding the level of detail of that information.

75. Some respondents raised concerns regarding the accuracy of the data recorded by biometric systems. Other comments inferred a concern about a lack of detail such as comments about “failure rates in fingerprint recognition” which would decline as the level of detail in recorded information increases. A response received from a software company puts forward the notion of limited accuracy as a virtue of the systems. This response states that the algorithms generated by the biometric systems they produce are accurate “to perhaps 1 in 30,000. This allows a high degree of certainty for comparisons within a small population such as a school, but no certainty when measured against a wider sample base. This inherent inaccuracy ensures that the data has no value outside the organisation in which it has been recorded.”

76. The level of detail contained in the information recorded by a biometric system is therefore a key consideration for an authority considering the implementation

of a biometric system. The technology should be able to record any information with a precision appropriate to the task for which it is to be used. Rather than a simple case for more detail being better, the precision of any system being considered should be appropriate to the size of the population intended for use. Too little detail could result in failures of the system to successfully fulfil its functions, too much detail would render the data more susceptible to security concerns.

77. There was no dispute among any commentators that the information recorded by a biometric system should be truthful. Nevertheless, we will consider the comments we did receive regarding the precision of information in the redrafting of the guidance.

Section 12. Access and use of data

Sample responses:

- "Access to the system must be on a need to know basis" (Information Commissioner's Office)

- "The consultation document does not make it clear whether any biometric system would be stand-alone in nature, or whether it would interface with schools' existing management information systems" (City of Edinburgh Council)

- "I know how technology can be used for good. I also know that the same technology can be used for other reasons." (Jackie Marshall)

78. Section 12 seeks to explain the need for clear procedures and rules restricting access to data, the importance of ensuring applications are self-contained, and also outlines some of a data-subject's rights under the Data Protection Act.

79. The response from the ICO makes the recommendation that "a record is kept of access in terms of who is accessing the system, when, how and why." Currently, this section of the draft guidance makes no recommendations about recording access. However, this is certainly consistent with the focus on good practice and we will consider inserting advice to this effect when the guidance is redrafted. They also state that "The ICO further recommends that the database is kept local to the school operating system."

80. A comment from the secondary education sector which was included in the response from a local authority states that "The consultation document does not make it clear whether any biometric system would be stand alone in nature". However, Paragraph 12.2 of the draft guidance states "Biometrics applications should be self-contained systems, whose templates cannot readily be used by computers running other fingerprint recognition applications."

Section 13. Retention

Sample responses:

- "data should be securely deleted/destroyed at the time the child permanently leaves the school for whatever reason. Furthermore, when a pupil enters secondary school, data collected at a feeder primary should not be transferred but new measurements should be taken." (Information Commissioner's Office)

- "Are there not legal statutes in place determining how long data is kept?" (Wester Cleddens Primary School, School Board)

81. Very few respondents commented on this section of the guidance. This section covers the need to develop a retention policy prior to the implementation of a biometric system and explains the implications of the Data Protection Act for data retention.

82. The ICO's response welcomes the emphasis placed on the development of a justified data retention policy and agrees with the statement in the guidance that "as soon as a pupil leaves the school, his/her biometric data would be immediately deleted."

83. The response received from a software company asserts that with the systems they have developed "Biometric data is destroyed after the student has left the school, ensuring that there is no record that can become accessible in the long term." This claim cannot, however, be made of biometric systems generally and the specifications of any system being considered should be scrutinised with regard to data retention and any justified data retention policy which has been developed.

84. Another response questioned a quoted section of the Data Protection Act which states that "Personal data processed for any purpose or purposes shall not be kept for any longer than is necessary for that purpose or those purposes." They questioned whether there were "legal statutes in place determining how long data is kept."

85. As the guidance is currently written, the relevant section of the legislation is quoted and it is for education authorities to take their own legal advice on how to comply with the legislation when formulating their own data retention policy. We are aware however, that the law with regard to data retention is of interest to data subjects as well as data controllers and we will consider whether a more complete statement of the legal requirements of the Act is necessary when the guidance is redrafted.

Sections 14, 15 & 16. Data protection policy, taking account of the needs of pupils with disabilities and critical risk management

Sample responses:

- "We think that the safeguards outlined in sections 10 (Security), 11 (Accuracy), 12 (Access and use of data), 13 (Retention), 14 (Data protection policy), 15 (Taking account of the needs of pupils with disabilities) and 16 (Critical risk management) are sensible. If these are followed, we see no problem with the use of safe biometric technologies for specific purposes." (Scottish Parent Teacher Council)

- "Back-up systems are a crucial component in enabling data controllers to comply with the seventh data protection principle and are of particular importance when a service is being accessed at the point of authentication in order to avoid undue distress to the service user." (Information Commissioner's Office)

86. Very few respondents commented directly on sections 14, 15 and 16 of the draft guidance. Where comments were received they were positive. We do not intend therefore to revise these sections.

Part 2: Other issues brought to our attention through the course of the consultation

87. This part of the report deals with issues which were raised in many of the responses but which fall outwith the scope of the consultation. Though the guidance seeks to address the issues which should be considered when electing to put in place a biometric system within a school, the recommendations which it makes operate within a pre-existing legislative framework. Though the concerns raised through this consultation represent an understandable and justified caution surrounding these technologies, we consider that through good practice and existing legislation, many of these issues can be alleviated. We, nevertheless, consider it proper to acknowledge some of these concerns as many of them raise issues which an authority should consider when contemplating the introduction of a biometric system, and where possible to address the issues they raise.

88. More than one response mentioned that there were aspects of biometric technologies which were considered to be "sinister". One respondent stated that "There is something quite sinister about palm scanning and fingerprint scanning" while another suggested that "The use of biometric technology is not something to be opposed per se, but many people feel instinctively that there is something sinister about fingerprinting children."

89. Concerns of this nature appear most frequently among the responses when discussing fingerprint scanning devices. There are less concerns raised in discussion of other types of biometric technology. This should not perhaps be surprising since, as another respondent pointed out, "biometrics - especially fingerprinting - has, an image traditionally and still associated with policing and criminal justice." This was acknowledged in the response we received from a software company, which suggested that "Much of the emotional content of this debate revolves around the comparison to the criminal overtone, and the fact that a biometric could be stolen as a form of identity theft."

90. The idea of introducing any kind of system into a school which gives the impression of criminalising children, even where it does not do so in reality, is something which will inevitably cause unease amongst parents. It is possible that this might be less of a concern with biometric systems which work through iris recognition or palm vein pattern analysis but, nevertheless, this should serve to underline the importance of involving parents and pupils in any decision to implement a biometric system. This will not only give parents and pupils the opportunity to voice concerns which may well influence decision making but will also give authorities an opportunity to discuss these concerns with parents who may find that many of them have been considered. It is for this reason that the draft guidance puts strong emphasis on the importance of consultation.

91. Another concern which was brought to our attention through responses to the consultation was that "Children and young people need to learn to handle money wisely, to know its value and to budget well." This concern, however, is true of all cashless systems and is not uniquely an issue for biometric technologies. Smart cards and pin number systems are as susceptible to this criticism as palm vein pattern recognition systems. Other reasons in favour of the use of cashless systems in schools remain unaffected and authorities should consider this issue with regard to their duty to reduce stigma under the Schools (Health Promotion and Nutrition) (Scotland) Act 2007.

Next Steps

92. The Principles Expert Group was established to advise the Scottish Government on high level principles on identity assurance and privacy for public services which are enabled by IT. Once the principles have been agreed we will revise and publish a final version of the guidance on biometric technologies in schools.

ISBN: 978-0-7559-7446-7

Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

Produced for the Scottish Government by RR Donnelley B59721

Published by the Scottish Government, February 2009

ISBN 978-0-7559-7446-7

9 780755 974467