|  |  |  |
| --- | --- | --- |
| **PS/David Laws****PS/Matthew Hancock**  | From:Tel:Date:Copy: | Chris ConnollyEducation Standards Management and Reducing Bureaucracy Division Ext 3380708 November 2012PS/ Secretary of StatePS/ Elizabeth TrussPermanent SecretarySpecial AdvisersStephen MeekJulie Bramman,+ list at end |

**PROTECTION OF BIOMETRIC INFORMATION OF CHILDREN IN SCHOOLS AND COLLEGES – PUBLICATION OF CONSULTATION RESPONSE AND UPDATED DRAFT DEPARTMENTAL ADVICE**

**Issue**

1. Finalising the departmental advice document for schools which use automated biometric recognition systems on the new duties in the Protection of Freedoms Act 2012, following a consultation on the draft advice.

**Recommendation**

2. That Ministers:

1. note the draft consultation report and government response attached at **Annex A** and agree to its publication; and
2. note the summary of the responses to the consultation at paragraphs 9 to 13 below and agree the minor changes to the final version of the Departmental advice document for publication. The draft advice is attached at **Annex B**.

**Timing**

3. Routine. However, a response by week commencing 19 November would allow us to publish the advice before the end of the autumn term.

**Background**

4. Biometric information is personal information about an individual’s physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements. This does not include photographs, other than where a photograph is scanned, for example for identifying biometric co-ordinates to provide someone with a service. The provisions apply to automated biometric recognition systems in use in schools such as automatic fingerprint identification, iris and retina scanning, and face recognition used to access catering, library or other services.

5. The Protection of Freedoms Act 2012 introduced new duties on schools and colleges that use automated biometric recognition systems that are expected to commence from 1 September 2013. They will apply to any school, sixth form college or further education institution where education is provided to children under 18. Sixth form colleges and 16-19 academies are covered by this DfE advice but separate advice has been made available by BIS via the Association of Colleges to cover FE institutions with under 18 students.

6. The new duties require schools and colleges to notify all parents that they intend to take and process their child’s biometric information. The written consent of at least one parent must be obtained before the data is taken from the child and used. In addition, a pupil can object or refuse to participate in the processing of his or her biometric information. Where pupils do not use the systems, either because their parents have refused consent or they themselves have refused to participate, schools are required to provide reasonable alternative arrangements for them.

7. Ministers previously cleared a draft departmental advice document for schools before it was issued for a 12 week consultation from 15 May to 3 August 2012. The aim of the consultation was to get feedback and publish final advice in good time for the new provisions coming into effect in September 2013.

**Argument**

**Response to the consultation and proposed changes to the advice document**

8. The consultation questions focused on whether the draft advice document was sufficiently clear in each area of its content. The changes we propose following the consultation do not impact substantially on the draft agreed earlier this year.

9. The consultation received 38 responses.  The responses were from a cross-section of schools, local authorities, suppliers and representative bodies including: The Children’s Food Trust and School Food Trust, The Independent Schools Council, ASCL, The National Governors’ Association, Association of Colleges, a provider of electronic systems, The Information Commissioner’s Office, NUT, Children’s Rights Alliance for England, The Boarding Schools Association, NAHT and Big Brother Watch.

10. Overall, the response to the draft advice was positive: 94% of respondents said that the explanations about biometric technology and processing were clear. 69% said that the advice about the notification and consent requirements was clear. 85% said that, having read the advice, they understood the new duties. A number of respondents suggested additions or clarifications for the ‘Frequently Asked Questions’ section of the advice. 55% agreed that the suggested notification and consent form template was clear enough for schools and families to understand and use and we are proposing to revise this in the final guidance as set out below.

11. Whilst not reflected generally in the consultation response or in further enquiries we have made with stakeholders, a supplier of biometric systems expressed concerns directly to us about the lead-in time for implementing alternative systems for their client schools (e.g. swipe cards). They have said that numbers of pupils who will not be participating in biometric systems are unanticipated both for those pupils about to be newly enrolled in a school and for those already attending and using these systems (for example, parents of pupils currently attending a school and already using a biometric system who may fail to provide written consent when notified under the new duties). Whilst we are clear that there will be no circumstances in which a school can lawfully process, or continue to process, a pupil’s biometric data without the necessary consents, we have strengthened the wording of the advice to highlight the need for schools to obtain the consents in advance of the duties coming into effect.

**Proposed changes**

12. For the final version of the advice, in addition to highlighting the need for schools to prepare for implementation as set out above, we have made a small number of clarification amendments in response to questions from the consultation, including: the definition of ‘parents’ in relation to obtaining consent; and the relationship between the new duties and the requirements of the Data Protection Act, for example on the use of CCTV and photographs in schools. We have also amended the suggested template notification letter for schools for clarification in response to comments. We have added the text to highlight that schools are free to adapt the letter in light of their own particular systems (and for example, the text may be adapted to notify parents of current pupils already using systems) but should ensure that parents are made aware of the requirements.

**Finance**

13. There are no financial implications as the advice for schools will be published on the DfE website.

**Presentation**

14. There is a clear need for advice in this area, given that the duties are new. It is envisaged that schools will welcome clarity and advice on the new legal duties they will need to fulfil if they use automated biometric recognition systems. We will ensure that schools are made aware of the advice when it is published as part of our termly communications with schools.

**Internal Clearance**

Julie Bramman (Director), Clare Simpson (Deputy Director, ESMRBD), Pam Charan (Legal Advisers Office).

Copy: Clare Simpson, Pam Charan, Carole Edge,

Patrick Heisel, Liam Flynn, Razeeb Ahasan, Charles Heymann, Richard Garbitz, Louise Baker, Dr Caroline Lucas (BIS).

**Annex A – draft Consultation Report and Government Response**



Analysis of responses to the consultation

Government response to the consultation

**Protection of biometric information of children in schools: consultation on draft advice for proprietors, governing bodies, head teachers, principals and school staff, young people, parents and representative bodies**

 **Consultation Unit**

**Department for Education**

 **Castle View House**

 **Runcorn**

 **Cheshire WA7 2GJ**

**Tel: 01928 794888**

 **x November 2012**

**Introduction**

The purpose of this consultation was to gather views on a Department for Education draft advice document intended to explain the legal duties schools and colleges have if they use automated biometric recognition systems.

Schools and colleges are increasingly making use of biometric identification systems, for example for attendance registration, cashless catering and site access. Biometric technologies are defined by the Information Commissioner as ‘*those which automatically measure people’s physiological or behavioural characteristics*.’ Examples of such systems in place in schools and colleges include automatic fingerprint recognition, iris and retina scanning, and face recognition.

In addition to the existing requirements under the Data Protection Act 1998, the provisions in the Protection of Freedoms Act 2012, which will come into force from **1 September 2013,** will apply to any school, sixth form college or further education institution where education is provided to children under 18.

Under the provisions in the Protection of Freedoms Act 2012 schools and colleges must notify the parents of pupils under 18 where they intend to use their child’s biometric data as part of an automated biometric recognition system. As long as the child does not object and no parent objects, the consent of only one parent will be required. Parental consent, objection or withdrawal of consent must be in writing. A pupil of any age may object or refuse to participate in an automated biometric recognition system. Where a parent has refused consent or a pupil has refused to participate, the school or college must provide reasonable alternative arrangements to the biometric system.

**The consultation sought feedback on the Department for Education’s draft advice document before publishing final advice in the 2012 autumn term, ahead of the duties in the Protection of Freedoms Act coming into force in September 2013. The consultation was open from** 14 May to 3 August 2012.

This report has been based on the 38 responses to the consultation document.

As some respondents may have offered a number of options for questions, total percentages listed under any one question may exceed 100%. Throughout the report, percentages are expressed as a measure of those answering each question, not as a measure of all respondents.

The organisational breakdown of respondents was as follows:

|  |  |  |
| --- | --- | --- |
| School/College Support Staff: | 10 | 26%  |
| Head teacher: | 5 | 13%  |
| Representative Body: | 5 | 13%  |
| Local Authority: | 3 | 8%  |
| Union: | 2 | 5%  |
| Voluntary Group: | 1 | 3%  |
| Teacher: | 1 | 3%  |
| Parent/Carer: | 1 | 3%  |
| Other – Please specify | 10 | 26% |
| **Total:** | **38** | **100%** |

*\*Those which fell into the ‘other’ category included: Big Brother Watch, Biostore Ltd, the Information Commissioner’s Office and the Children’s Food Trust and School Food Trust.*

The report starts with an overview, followed by a summary analysis of each question within the consultation.

**Overview of responses**

|  |
| --- |
| **1 Do you find the explanations in sections 1-3 of the advice about what is meant by "biometric data technology" and "processing" clear enough?** |
| There were **33** responses to this question |
| **Options** | **Responses** | **Across Consultation** |
| Yes: | 31 | 94%  | 82%  |
| No: | 1 | 3%  | 3%  |
| Not Sure: | 1 | 3%  | 3%  |
| **2 Do you think the advice in sections 4-6 setting out the notification and consent requirements and the pupil's right to object is sufficiently clear?** |
| There were **35** responses to this question |
| **Options** | **Responses** | **Across Consultation** |
| Yes: | 24 | 69%  | 63%  |
| No: | 9 | 26%  | 24%  |
| Not Sure: | 2 | 6%  | 5%  |
| **3 Having read the advice document, do you understand the legal duties on schools and sixth form colleges?** |
| There were **33** responses to this question |
| **Options** | **Responses** | **Across Consultation** |
| Yes: | 28 | 85%  | 74%  |
| No: | 3 | 9%  | 8%  |
| Not Sure: | 2 | 6%  | 5%  |
| **4 Is there anything you think we could usefully add to the ‘Frequently Asked Questions' section of the document?** |
| There were **32** responses to this question |
| **Options** | **Responses** | **Across Consultation** |
| Yes: | 19 | 59%  | 50%  |
| No: | 9 | 28%  | 24%  |
| Not Sure: | 4 | 13%  | 11%  |
| **5 Do you think the notification and consent form template is clear enough for schools and families to understand and use?** |
| There were **31** responses to this question |
| **Options** | **Responses** | **Across Consultation** |
| Yes: | 17 | 55%  | 45%  |
| No: | 10 | 32%  | 26%  |
| Not Sure: | 4 | 13%  | 11%  |

The majority of respondents felt that the draft advice was sufficiently clear in explaining biometric data technology, the processing of biometric information and the new duties on schools using or planning to use these systems.

As set out in detail in the Summary and Responses section below, a number of respondents felt that some specific areas of the draft advice would benefit from clarification and we will aim to address these in the final version of the advice.

Whilst most respondents felt that the advice is helpful, 32% of respondents said that the notification and consent form template is not clear enough for schools and families to understand and use (Question 5). As set out in the summary, schools can adapt the template, as appropriate, to their own particular circumstances and we will aim to clarify this in the final advice document.

**Summary and Responses**

**Q1) Do you find the explanation in sections 1-3 of the advice about what is meant by “biometric data technology” and “processing” clear enough?**

**There were 33 responses to this question**

Yes 31 94% No 1 3% Not Sure 1 3%

The majority of respondents felt that the explanations given for the meanings of biometric data, biometric recognition technology and the processing of biometric information were sufficiently clear.

A number of respondents suggested that further clarification may be required on the status of photographs in relation to biometric data. The reference to photographs in Section 1 1) of the draft advice will be removed and clarified within the ‘Frequently Asked Questions’ section of the advice document to explain that the use of photographs and CCTV generally (i.e. other than for the purposes of an automated biometric recognition system) is governed by the Data Protection Act 1998.

A few respondents queried the explanation of processing data in relation to recording, storing and using that data. Paragraph 3 1) of the draft advice on data processing will be amended to set out that data processing takes place when any of the processes listed at a. b. and c. take place, clarifying that not all three need to occur for processing to take place.

**Q2) Do you think the advice in sections 4-6 setting out the notification and consent requirements and the pupil's right to object is sufficiently clear?**

**There were 35 responses to this question**

Yes 24 69% No 9 26% Not Sure 2 6%

A number of respondents suggested that the advice in these sections could be clearer on the requirements on schools for notifying and obtaining consent from parents and the definition of parent in relation to the duties in the Protection of Freedoms Act 2012. These paragraphs will be redrafted to reflect this.

A number of respondents expressed the view that the paragraph in the draft advice setting out that schools should take steps to ensure pupils understand that they can object to having their biometric data processed could be strengthened to make sure that pupils are aware of their rights in relation to their biometric data, including that the information given to pupils should take into account the child’s age and understanding. Reference to this will be added to the advice.

A few respondents suggested that the advice document should include information on how processing biometric data relates to the schools’ Privacy Notices issued to pupils. The final advice document will set out that, in addition to the required actions for notification and obtaining consent, schools may wish to include information in the Privacy Notices they issue to pupils about the requirements and explaining how biometric information is processed and stored by the school. The advice document will provide a link to the DfE guidance on Privacy Notices.

**Q3) Having read the advice document, do you understand the legal duties on schools and sixth form colleges?**

**There were 33 responses to this question**

Yes 28 85% No 4 9% Not Sure 2 6%

Most respondents agreed that the draft advice enabled them to understand the duties on schools in the Protection of Freedoms Act 2012.

A number of respondents expressed the view that the draft advice did not include information on the advantages and benefits of such systems for pupils and schools. This is outside of the scope of the DfE advice on the duties in the Protection of Freedoms Act 2012 and we would expect schools to enable parents and pupils to make informed decisions about participating in the automated biometric recognition system in this context.

A few respondents were concerned about the practicalities of implementation, setting out that where a system is already in place in a school, some parents of pupils currently attending the school and using the biometric system may fail to provide consent when notified under the new duties. It was suggested that schools could take failure to respond as consent in these circumstances. The Protection of Freedoms Act 2012 does not provide for this suggestion and requires active consent from parents in writing. The advice document will be amended to include clarification about the introduction of the new duties, clarifying the fact that there will be no circumstances in which a school or college can lawfully process a pupil’s biometric data without having received the necessary written consent.

**Q4) Is there anything you think we could usefully add to the ‘Frequently Asked Questions' section of the document?**

**There were 32 responses to this question**

Yes 19 59% No 9 28% Not Sure 4 13%

A number respondents suggested that the draft FAQ on the use of photographs and CCTV in schools could be clarified to explain the additional requirements in the Protection of Freedoms Act relating to biometric information used as part of an automated biometric recognition system and the requirements in the Data Protection Act which apply to the processing of all biometric information, including the taking, use and storage of photographs and the operation of CCTV in schools and colleges for whatever purposes. This FAQ will be amended in the advice document to reflect these distinctions.

Some respondents felt that further explanation should be given on how the biometric data might actually be collected, for example that an actual fingerprint may not be retained but a mathematical algorithm of the data, or a number of points of that data, which could not be ‘reverse engineered’ into a fingerprint image. While a full explanation of the range of systems in use is outside the scope of the advice document, we would expect schools to provide these explanations to parents and pupils as an element of notification and consent. However, a footnote will be added to section 3 of the advice document ‘What does processing data mean’, which will include the example of the measurements from fingerprints being converted into a template.

**Q5) Do you think the notification and consent form template is clear enough for schools and families to understand and use?**

**There were 31 responses to this question**

Yes 17 55% No 10 32% Not Sure 4 13%

A number of respondents felt that the template notification letter and consent form do not go far enough in explaining the benefits and advantages of biometric systems or the services provided by the systems or what schools hope to achieve by using the technology. It is outside the scope of the template letter provided in the DfE advice to include this kind of information. The template is intended as a suggested letter and schools may adapt it or provide their own letter. However, as set out in the template, schools must notify parents and provide sufficient information for the parents to make an informed decision; this should include the school’s duty to make reasonable alternative arrangements if the child or parent does not agree to the processing.

Some respondents said that the template notification letter and consent form are complex and will not be understood by many readers. As set out above, schools are free to adapt the suggested template and produce their own material appropriate to the requirements.

The template will be retained in the advice and amended to provide a clear outline of what should be included in the notification to parents which schools may adapt.

 **Next Steps**

The Department for Education will publish a revised version of the advice document by the end of the autumn term 2012.

DfE will monitor the impact of the introduction of the new duties on schools and review the advice document in future years.

**Annex B – Draft Advice Document**

PROTECTION OF BIOMETRIC INFORMATION OF CHILDREN IN SCHOOLS

Advice for proprietors, governing bodies, head teachers, principals and school staff

**About this advice**

This is non-statutory advice from the Department for Education. It is intended to explain the legal duties schools and sixth-form colleges have if they wish to use biometric information about pupils for the purposes of *automated biometric recognition systems*.

**The duties on schools in the Protection of Freedoms Act 2012 set out in this advice come into effect from 1 September 2013.**

**Schools and colleges using automated biometric recognition systems or planning to install them are advised to plan, in advance, to make arrangements to notify parents and obtain the consent required under the new duties as set out in the body of this advice. This will be particularly relevant for schools where pupils are already enrolled and using automated biometric recognition systems. There will be no circumstances in which a school or college can lawfully process, or continue to process, a pupil’s biometric data without having notified each parent of a child and received the necessary consent after the new duties come into effect.**

This advice replaces “*Becta guidance on biometric technologies in schools”.*

Sixth form colleges and 16-19 Academies are covered by this advice. Separate advice will be issued by the Department for Business, Innovation and Skills to cover FE institutions with students under 18 years of age.

**Expiry/review date**

This advice will be kept under review and updated as necessary.

**What legislation does this advice relate to?**

The Protection of Freedoms Act 2012

The Data Protection Act 1998

**Who is this advice for?**

This advice is aimed at proprietors, governing bodies, head teachers and principals of **all** schools[[1]](#footnote-1), sixth form colleges and 16-19 Academies. It will also be of use to school and college staff, parents and pupils.

**Key points**

* Schools and colleges that use pupils’ **biometric data** (see 1 below) must treat the data collected with appropriate care and must comply with the data protection principles set out in the Data Protection Act 1998.
* Where the data are to be used as part of an **automated biometric recognition system** (see 2 below), schools and colleges must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012 (see **Protection of Freedoms Act 2012** below).
* Schools and colleges must ensure that each parent of a child is notified of the school’s intention to use the child’s **biometric data** (see 1 below) as part of an automated biometric recognition system.
* The written consent of at least one parent must be obtained before the data are taken from the child and used (i.e. **‘processed’** – see 3 below). This applies to all pupils in schools and colleges **under the age of 18.** In no circumstances can a child’s biometric data be processed without written consent.
* Schools and colleges must not process the biometric data of a pupil (under 18 years of age) where:
	1. the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
	2. no parent has consented in writing to the processing; or
	3. a parent has objected in writing to such processing, even if another parent has given written consent.
* Schools and colleges must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

**1 What is biometric data?**

1. *Biometric data* means personal information about an individual’s physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.
2. The Information Commissioner considers all biometric information to be personal information under the Data Protection Act 1998; this means that it must be obtained, used and stored in accordance with that Act (see the **Data Protection Act 1998** below).
3. The Protection of Freedoms Act includes provisions which relate to the use of biometric data in schools and colleges when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the Data Protection Act 1998. (See the **Protection of Freedoms Act 2012** below).

**2 What is an automated biometric recognition system?**

1. An *automated biometric recognition system* uses technology which measures an individual’s physical or behavioural characteristics[[2]](#footnote-2) by using equipment that operates ‘automatically’ (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual.
2. Biometric recognition systems can use many kinds of physical or behavioural characteristics such as those listed in **1**, 1) above.

**3 What does processing data mean?***‘Processing’* of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including disclosing it, deleting it, organising it or altering it.[[3]](#footnote-3)An automated biometric recognition system processes data when:

1. 1. recording pupils’ biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
	2. storing data relating to pupils’ biometric information on a database system; or
	3. using the data as part of an electronic process**,** for example, by comparing it withbiometric information stored on a database in order to identify or recognise pupils.
2. More information on these topics is available via the **Associated Resources** section below.

**THE PROTECTION OF FREEDOMS ACT 2012**

**4 Notification and Parental Consent**

*What the law says:*

1. Schools and colleges **must** notify **each** parent[[4]](#footnote-4) of a pupil under the age of 18 if they wish to take and subsequently use the child’s biometric data as part of an automated biometric recognition system.
2. As long as the child or a parent does not object, the written consent of only one parent will be required for a school or college to process the child’s biometric information. A child does not have to object in writing but a parent’s objection must be written.
3. Schools and colleges will not need to notify a particular parent or seek his or her consent if the school or college is satisfied that:

	1. the parent cannot be found, for example, his or her whereabouts or identity is not known;
	2. the parent lacks the mental capacity[[5]](#footnote-5) to object or to consent;
	3. the welfare of the child requires that a particular parent is not contacted, for example where a child has been separated from an abusive parent who is not to be informed of the child’s whereabouts; or
	4. where it is otherwise not reasonably practicable for a particular parent to be notified or for his or her consent to be obtained.
4. Where none of the parents of a child can be notified for one of the reasons set out above (which would mean consent cannot be obtained from any of them), section 27 of the Protection of Freedoms Act 2012 sets out who should, in such circumstances, be notified and who can give consent:

(a) if the child is being ‘looked after’ by a local authority[[6]](#footnote-6) or is accommodated or maintained by a voluntary organisation (i.e. a not-for-profit organisation), the local authority, or as the case may be, the voluntary organisation must be notified and their consent written consent obtained.

(b) if paragraph (a) above does not apply, then notification must be sent to all those caring for the child and written consent must be gained from at least one carer before the child’s biometric data can be processed (subject to the child and none of the carers objecting in writing).

1. There will never be any circumstances in which a school or college can lawfully process a child’s biometric information (for the purpose of an automated biometric recognition system) without one of the persons above having given written consent.
2. Under the Education (Pupil Registration) Regulations 2006, schools are required to keep an admissions register that includes the name and address of every person known to the school to be a parent of the child, including non-resident parents. Schools that wish to notify and seek consent to process a child’s biometric information at any point after the enrolment of a child at the school should, therefore, have contact details for most parents in the admission register.
3. Schools should, however, be alert to the fact that the admission register may, for some reason, not include the details of both parents. Where the name of only one parent is included in the admission register, schools should consider whether any reasonable steps can or should be taken to ascertain the details of the other parent, for example, by asking the parent who is included in the admission register or, where the school is aware of local authority or other agency involvement with the child and its family, by making enquiries with the local authority or other agency.  Schools and colleges are not expected to engage the services of ‘people tracer’ or detective agencies in doing so but are expected to take reasonable steps to locate a parent before they are able to rely on the exemption in section 27(1)(a) (notification of a parent not required if the parent cannot be found).
4. An option would be for schools and colleges to notify parents that they intend to take and then use their child’s biometric information as part of an automated biometric recognition system and seek written consent to do so at the same time as obtaining details of parents as part of the enrolment process. In other words, details of both parents would be requested by the school or college for both purposes (enrolment and notification of intention to process biometric information).
5. Notification sent to parents should include full information about the processing of their child’s biometric information. This information should include: details about the type of biometric information to be taken; how it will be used; the parents’ and the pupil’s right to refuse or withdraw their consent; and the school’s duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed. A suggested sample ‘Notification and Consent’ template is included at the end of this advice.

**5 The pupil’s right to refuse**

*What the law says:*

1. If a pupil of any age under 18 objects or refuses to participate (or to continue to participate) in anything that involves the processing of their biometric data for the purposes of an automated biometric recognition system, the school or college **must** ensure that the pupil’s data **are not** processed. The child’s objection or refusal overrides any parental consent to the processing.

*Also note:*

1. Schools and colleges should take steps to ensure that pupils understand that they can object or refuse to allow their biometric data to be used and that, if they do so, the school or college will have to provide them with an alternative way of accessing the relevant service. The steps taken to inform children should take account of their age and understanding. Parents should also be told of their child’s right to object or refuse and encouraged to discuss this with their child.
2. In addition to the required actions for notification and obtaining consent, schools may wish to include information in the Privacy Notices to be issued to pupils about the requirements and explaining how biometric data are processed and stored by the school. Further advice and suggested templates for Privacy Notices for schools can be found on the Department for Education website <http://www.education.gov.uk/researchandstatistics/datatdatam/a0064374/suggested-text-and-guidance-for-issuing-privacy-notices>

**6 Providing alternatives**

*What the law says:*

1. Reasonable alternative arrangements must be provided for pupils who do not use automated biometric recognition systems either because their parents have refused consent (or a parent has objected in writing) or due to their own refusal to participate in the collection of the biometric data.
2. The alternative arrangements should ensure that children do not suffer any disadvantage or difficulty in accessing services/premises, etc as a result of them not participating in an automated biometric recognition system. Likewise, such arrangements should not place any additional burden on parents whose children are not participating in such a system.

**THE DATA PROTECTION ACT 1998**

1. Schools and colleges as *data controllers* must process pupils’ personal data, including biometric data, in accordance with the Data Protection Act 1998 (DPA). The provisions in the Protection of Freedoms Act 2012 are in addition to the requirements in the DPA with which schools and colleges must continue to comply.
2. The DPA has eight principles with which all data controllers must comply. *More details on each of these principles can be found through the* ***Associated Resources*** *section below.*
3. When processing a child’s personal data, including any such data used for the purpose of automated biometric recognition systems, schools and colleges must comply with these principles, including:

	1. Holding biometric data *securely* to prevent unauthorised or unlawful use of the data.
	2. Storing biometric data *for no longer than it is needed*. A school or college must, therefore, destroy any data held on a biometric system once a pupil no longer uses the system. For example, the data should be destroyed if the pupil leaves the school or college, if parents withdraw consent or the child no longer wishes to have his or her biometric data processed.
	3. Ensuring that such data are *used only for the purposes for which it is obtained* and that it is not *unlawfully* disclosed to third parties.
	4. For further practical advice see the **Associated Resources** section below.

**Frequently Asked Questions**

**What information should schools provide to parents/pupils to help them decide whether to object or for parents to give their consent?**

Any objection or consent by a parent should of course be an informed decision – as should any objection on the part of a child. Schools and colleges should take steps to ensure parents receive full information about the processing of their child’s biometric data including a description of the kind of system they plan to use, the nature of the sensitive data they process, the purpose of the processing and how the data will be obtained and used. Children should be provided with information in a manner that is appropriate to their age and understanding.

**What if one parent disagrees with the other?**

Schools and colleges will be required to notify each parent of a child that they intend to take and process the child’s biometric information. If one parent objects in writing, then the school or college will not be permitted to process the child’s data.

**How will the child’s right to object work in practice – must they do so in writing?**

A child is not required to object in writing. An older child may be more able to say that they object to the processing of their biometric data. A younger child may show reluctance to take part in the physical process of giving the data in other ways. In either case the school or college will not be permitted to collect or process the data.

**Are schools required to ask/tell parents before introducing an automated biometric recognition system?**

The law doesn’t require that parents are consulted before an automated biometric recognition system is installed, only that parents be notified and that consent from at least one parent be gained before their child’s biometric data is obtained or used for the purposes of such a system. It is up to schools to decide whether they think it is appropriate to consult parents and pupils in advance.

**Do schools need to renew consent every year?**

No. The original written consent is valid until such time as it is withdrawn. However, it can be overridden, at any time, if another parent or the child objects to the processing (subject to the parent’s objection being in writing). When the pupil leaves the school, their data should be removed from the school’s system.

**Can consent be withdrawn by a parent?**

Parents will be able to withdraw their consent, in writing, at any time. In addition, either parent will be able to object to the processing at any time but they must do so in writing.

**When and how can a child object?**

A child can object to the processing or refuse to take part at any stage – i.e. before the processing takes place or at any point after his or her biometric data has been obtained and is being used as part of a biometric recognition system. If the child objects, the school or college must not start to process his or her data or, if they are already doing so, must stop doing so. The child does not have to object in writing.

**Will consent given on entry to primary or secondary school be valid until the child leaves that school?**

Yes. Consent will be valid until the child leaves the school – subject to any subsequent objection to the processing of the data by the child or a written objection from a parent. If any such objection is made, the data should not be processed (or should stop being processed) and the school or college must, in accordance with the Data Protection Act principles, remove it from the school’s system.

**Can the school notify parents and accept consent via email?**

Yes – as long as the school is satisfied that the email contact details are accurate and the consent received is genuine.

**Will parents be asked for retrospective consent?**

No. Any processing that has taken place prior to the provisions in the Act coming into force will not be affected. However, from 1 September 2013 (when the new duties in the Protection of Freedoms Act take effect),any school or college wishing to continue to process the biometric data of pupils for the purposes of an automated biometric recognition system must**,** before that date, havesent the necessary notifications to each parent of a child and obtained the written consent from at least one parent before continuing to use the child’s biometric data as part of such a system.

**Does the legislation cover other technologies such a palm and iris scanning?**

Yes it does. The legislation covers all systems that record or use physical or behavioural characteristics for the purpose of identification. This will include systems which use palm, iris or face recognition amongst others, as well as fingerprints.

**Is parental notification and consent under the Protection of Freedoms Act 2012 required for the use of photographs and CCTV in schools?**

No – not unless the use of photographs and CCTV is for the purposes of an automated biometric recognition system. However, schools and colleges must continue to comply with the requirements in the Data Protection Act 1998 when using CCTV on their premises for general security purposes or when using photographs of pupils as part of a manual ID system or as part of an automated system that uses a barcode to provide a child with access to services. Depending on the circumstances of each case, consent may be required or be advisable under the Data Protection Act provisions. The Government believes that the Data Protection Act requirements are sufficient to regulate the use of CCTV and photographs for purposes other than automated biometric recognition systems.

Photo ID card systems where a child’s photo is scanned automatically, for example, to provide him or her with services would come within the obligations on schools and colleges in sections 26 to 28 of the Protection of Freedoms Act 2012 as such systems fall within the definition in that Act of automated biometric recognition systems.

**Is parental notification or consent required where a child uses or accesses standard commercial sites or software which use face recognition technology?**

The provisions in the Protection of Freedoms Act 2012 only cover processing by or on behalf of a school or college. If a school or college wishes to use such software for school work or any school business, then the requirement to notify parents and to obtain written consent will apply. However, if a pupil is using this software for their own personal purposes then the provisions do not apply, even if the software is accessed using school or college equipment.

**Associated Resources**

DfE guidelines for schools on communicating with parents and obtaining consent:

<http://www.education.gov.uk/schools/pupilsupport/parents/a0014568/parental-responsibility>

ICO guide to data protection:<http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx>

ICO guidance on data protection for education establishments: <http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx>

British Standards Institute guide to biometrics: <http://shop.bsigroup.com/en/Browse-by-Subject/Biometrics/?t=r>

**Template Notification and Consent Form**

The following is an optional notification letter and consent form for schools to use to notify parents. Schools may wish to adapt the text in light of their own particular systems (and for example, the text may be adapted to notify parents of current pupils already using systems) but should ensure that parents are made aware of the requirements of sections 26-28 of the Protection of Freedoms Act 2012 as set out.

**NOTIFICATION OF INTENTION TO PROCESS PUPILS’ BIOMETRIC INFORMATION**

**Dear *[name of parent/carer]***

The school *[college]* wishes to use information about your child as part of an automated (i.e. electronically-operated) recognition system. This is for the purposes of *[specify what purpose is – e.g. catering, library access?]*. The information from your child that we wish to use is referred to as ‘biometric information’ (see next paragraph). Under the Protection of Freedoms Act 2012 (sections 26 to 28), we are required to notify each parent of a child and obtain the written consent of at least one parent before being able to use a child’s biometric information for an automated system.

**Biometric information and how it will be used**

*Biometric information* is information about a person’s physical or behavioural characteristics that can be used to identify them, for example, information from their [*fingerprint/iris/palm*]. The school would like to take and use information from your child’s [*insert biometric to be used*] and, as stated above, use this information for the purpose of providing your child with *[specify what purpose is]*.

The information will be used as part of an automated biometric recognition system. What this system will do is take measurements from your child’s [*insert biometric to be used]* and convert these measurements into a template that is stored on the system. An image of your child’s *[insert biometric]* is not stored. The template is what will be used in order to identify or recognise your child when accessing services*.*

You should note that the law places specific requirements on schools *[colleges]* when using personal information, such as biometric information, about pupils. For example:

(a) the school *[college] cannot* use the information for any purpose other than the one it was obtained for (stated above);

(b) the school *[college]* must ensure that the information is stored securely;

(c) the school *[college]* must tell you what it intends to do with the information;

(d) the school *[college]*cannot disclose it unlawfully to any other person – you should note that the only person that the school wishes to share the information with is *[insert any third party with which the information is to be shared e.g X supplier of biometric systems]*. This is necessary in order to *[say why it needs to be disclosed to the third party]*.

**Providing your consent/objecting**

As stated above, in order to be able to use your child’s biometric information in this way, the written consent of at least one parent is required. However, you should note that consent given by one parent is overridden if another parent objects in writing to the use of the information. In addition, if the child objects or refuses to use the biometric recognition system, the school *[college]* cannot use your child’s information.

You can, therefore, object, in writing, to the proposed processing of your child’s biometric information now or at any later stage or, if you consent, you can withdraw this consent at any time. Please note that any consent or objection from you or any other parent must be in writing.

In addition, your child may at any time object or refuse to allow their biometric information to be used even if you have given your consent. *[His/her]* objection does not need to be in writing. We would appreciate it if could you discuss what is intended with your child and explain to them that they can object if they wish to do so.

The school *[college]* is also happy to answer any questions you or your child may have.

If you do not wish your child’s biometric information to be processed by the school, or your child objects to such processing, the law says that we must provide reasonable alternative arrangements that allow your child and any other child at the school who is not going to use the automated system to [*insert relevant service e.g. access school library*].

Should you, however, be willing to agree to the processing of your child’s biometric information, please could you sign, date and return the consent form below to the school.

Please note that when your child leaves the school, or if for some other reason he/she ceases to use the biometric system, his/her biometric data will be deleted.

**Further information and guidance**

This can be found via the following links:

Department for Education’s ‘*Protection of Biometric Information of Children in Schools – Advice for Governing bodies, head teachers, Principals and school staff’* [**New link to be added when available**]

ICO guide to data protection: <http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx>

ICO guidance on data protection for education establishments: <http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx>

**CONSENT FORM FOR SCHOOLS - USE OF BIOMETRIC DATA**

Please complete the form below and sign and date it if you consent to information from your child’s *[insert biometric – e.g. fingerprint]* being used by the school *[college]* as part of an automated biometric recognition system for *[describe purpose data will be used for e.g. administration of school library/ canteen ]*until your child leaves the school or for some other reason no longer uses such a system. Please note that when your child leaves the school, or if for some other reason he/she ceases to use the biometric system, his/her biometric data will be deleted.

**Name of the child**…………………. ……

**Name of Parent …………………………………………………………………………..**

**Signature of Parent**

**Date………………………………………………………………………………**

1. This includes Academies, Free Schools, other types of independent schools, maintained schools and non-maintained special schools. [↑](#footnote-ref-1)
2. Biometric systems usually store measurements taken from a person’s physical/behavioural characteristics and not images of the characteristics themselves. For example, a fingerprint image is not stored on the system but measurements from the fingerprint are converted into a template and the template is stored. The templates are also biometric data. [↑](#footnote-ref-2)
3. See section 1(1) of the Data Protection Act 1998. [↑](#footnote-ref-3)
4. The parents of a child include not only the biological mother or father (or the adoptive parents) but any other individual with parental responsibility for the child. Part 1 of the Children Act 1989 setsout who has parental responsibility and what this means. [↑](#footnote-ref-4)
5. Within the meaning of the Mental Capacity Act 2005 [↑](#footnote-ref-5)
6. For example, the child is subject to a care order in favour of the local authority or the local authority provides accommodation for the child – see section 22 of the Children Act 1989 for the definition of ‘looked after’ child. [↑](#footnote-ref-6)