

Privacy Impact Assessment

The following document outlines the tasks required to produce a privacy impact assessment for schools who wish to implement a biometric system for attendance. The privacy impact assessment should be carried out before schools install the biometric system.

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

- If the introduction of a biometric system is justified, can I offer an alternative system to individuals who may object to the invasion of privacy involved in a biometric system?
- What is my retention policy on biometric data?
- Can I justify the retention period in my retention policy?
- How shall I inform students about the system?
- What information about the system need I provide to students?
- Would I be happy if I was a student asked to use such a system?
- Am I happy to operate a biometric system in an educational establishment where the use of such a system can make students less aware of the data protection risks that may impact upon them in later life?
- Does my school or college have a comprehensive data protection policy as required by the Department of Education and Science since 2003?
- Have I updated this policy to take account of the introduction of a biometric system for use by students?