

ICO Guidance

The use of biometrics in schools

This is a brief statement of the Commissioner's view on the use of biometric technologies in schools.

Biometric technologies are those which automatically measure people's physiological or behavioural characteristics. Examples include automatic fingerprint identification, iris and retina scanning, face recognition and hand geometry, and their use is becoming increasingly common in both public and private sectors.

Schools have over the last few years begun to use automated fingerprint identification systems (AFIS) for registration, library book borrowing and cashless catering. Fingerprints are not essential to the applications but unlike swipe cards they cannot be lost, and this has been given as a reason for using them. A subset of the unique features of the fingerprint are extracted from a scanned image and converted into a biometric "template". This template, a binary number, is checked against the template generated each time a person places his finger on the scanner. Full fingerprint images are not stored and cannot be generated ("reverse engineered") from the template.

One objection to fingerprinting in schools is that it stigmatises those who have their fingerprints taken. It is felt to be indicative of mistrust and suspicion and is identified with being "treated like criminals". The opposition is thus based on the other uses associated with the method, rather than the circumstances of the present use. Others are concerned that fingerprinting in schools will teach children that giving up important personal information, and particularly biometrics, to those in authority is perfectly routine and mundane. It has even been suggested that fingerprinting in schools is part of a concerted attempt to "soften up" the younger generation for increased state privacy intrusion, including initiatives such as ID cards and DNA testing. Any use of biometric technologies outside law enforcement should be considered in the light of such negative responses. However, these concerns, while raising wider questions of public attitude and public policy, are not specifically data protection issues.

Despite the connotations of fingerprinting, it is impossible to say that the use of fingerprints outside law enforcement, for instance where entitlement to services is involved, will inevitably breach the Data Protection Act ("the Act"). But certain features of such systems will make them more or less likely to be acceptable on privacy and security grounds. It is important that the information is only used for purposes specified when it is collected. For this reason biometrics applications should be self-contained systems, whose templates cannot readily be used by computers running other fingerprint recognition applications. The key issue is "interoperability": the use of information across different systems. Even where systems were developed locally, interoperable technologies could allow them to be linked. This could enable the construction of *de facto* fingerprint databases of large parts of the population. In our view such an enterprise should only be

introduced when explicitly authorised by the Government and subject to public debate and appropriate legislation.

The numeric template information held for school biometrics systems would also be a more attractive target for theft in circumstances where it could be used in other applications, or where full fingerprint images could be obtained from the templates. If interoperable biometric systems were in common use for identification purposes, the consequences of the loss of one's fingerprint template could be severe. It should be appreciated by those operating biometric systems that high standards of security will be needed to safeguard them. Biometric data must also be destroyed when it is no longer needed.

There is a great deal of confusion around the role of consent. It has been widely supposed that it must be illegal for schools to collect pupils' fingerprints without their parents' consent. There are two issues here. First of all there is a common misconception that all processing of personal data must take place on the basis of consent. This is not the case. (In the enrolment phase of school fingerprinting children will obviously have to cooperate by placing their finger on the scanner, but this cannot be regarded as consent to the wider use of their print unless they have been fully informed about it.) Second, there is nothing in the Act that states that until a child reaches a specific age any data protection rights they have should be exercised by their parents or guardian. For the purposes of the Act the pupils themselves are "data subjects": it is they who should in the first instance be informed and consulted about the use of their personal data. Deciding when children are mature enough to decide how their personal information should be used is difficult. On the one hand, as children mature they are entitled to an increasing measure of autonomy. On the other hand, while children might understand a simple explanation of why their fingerprints are being taken, they may well not appreciate the potential wider implications.

There is nothing explicit in the Act to require schools to seek consent from all parents before implementing a fingerprinting application. However, unless schools can be certain that all children understand the implications of giving their fingerprints, they must fully involve parents in order to ensure that the information is obtained fairly. Parents play a central role in their children's education, in terms of support and guidance, and also in terms of legal liability, for example in case of truancy. They therefore rightly expect to be informed and consulted when biometric systems are introduced in their child's school. Suspensions are only likely to be increased when new and possibly controversial technology is introduced without a comprehensive effort to address people's fears and concerns.

Schools should explain the reasons for introducing the system, and how personal data is used and kept safe. In view of the sensitivity of the issue and the importance of parents' role in education it would also be a heavy-handed approach for schools not to respect the wishes of those pupils and parents who

object to school fingerprinting initiatives. This is especially pertinent given the flexibility of systems such as Junior Librarian, where a card can work just as well as a fingerprint, so that those who wish to “opt out” can be given another means of accessing the same services.

Appendix: The data protection principles

The Data Protection Act 1998 includes eight data protection principles with which data controllers must comply. The first, second, fifth and seventh principles are the most relevant to this issue.

The first principle requires that personal data is processed fairly and lawfully. Fairness requires that schools ensure that pupils are informed about and understand the purpose for which their personal data is being processed.

The second principle requires that personal data is obtained for one or more specified and lawful purposes and not further processed in any manner incompatible with that purpose or those purposes. Children’s biometric data should therefore not be used for any purpose not directly related to that for which it was collected.

The fifth principle requires that personal data is not kept for longer than it is needed for its specified purpose. Pupils’ biometric data should therefore be destroyed when they have left the school.

The seventh principle requires that appropriate security is in place to safeguard personal data from unauthorised processing and accidental loss, destruction or damage.