B20

USE OF BIOMETRIC DATA

(Data Protection)

Reference Points

- Data Protection Act 1998
- Protection of Freedoms Act 2012
- *Protection of Biometric Information of Children in Schools: Advice for proprietors, governing bodies, head teachers, principals and school staff,* December 2012 https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools
- See also in this Handbook 'Section B06 – Data Protection Matters – DPA Model Policy'

Contact Point

Amy Hall - Principal Legal Officer (Commercial and Information Governance)
Tel: 01522 552039
Email: amy.hall@lincolnshire.gov.uk

Amy Jaines - Principal Legal Officer (Commercial and Information Governance)
Tel: 01522 552553
Email: amy.jaines@lincolnshire.gov.uk

School Liaison Officer (01522 554884)

Schools are beginning to use biometric data such as fingerprint technology to run cashless lunch queues, school libraries and attendance systems. It frees up teacher time and makes day-to-day administration easier. It can help to remove stigma for pupils receiving free school meals and means that schools don't have the problems associated with loss and replacement of other forms of identification. It helps in preventing unauthorised access to school premises and can help to identify when particular pupils are not attending lessons, prompting more immediate action.

This guidance is to highlight the key points to headteachers and governing bodies regarding the action they need to take in order to comply with the law when using these technologies and the need to be clear and open with all parents and pupils about the following:

- what the technology is
- how it will be used
- why it is required
- what is involved
- what data will be held and stored

- how long it will be secured and held

For detailed advice, frequently asked questions and letter templates, schools are directed to the DfE guidance document *Protection of Biometric Information of Children in Schools: Advice for proprietors, governing bodies, head teachers, principals and school staff (*December 2012). A link is provided under Reference Points above.

Action Points

- Schools are advised to recognise some parents' or pupils' concerns over the introduction of biometric systems and must offer alternative systems, such as smartcards, to access the same services if they want to opt out.

- The Data Protection Act requires that:
  - schools cannot use biometric information other than for the express purpose for which it is collected, i.e. data taken for use in a school library, can only be used for that purpose;
  - schools must process all personal data fairly and lawfully, i.e. all pupils and their parents must be told what personal information is on record and how it is intended to be used;
  - schools cannot pass on biometric information to any outside agencies, nor can third parties access this information;
  - schools cannot keep personal data for longer than it is needed for its specific purpose. Pupils' biometric data should therefore be destroyed when they have left the school.
  - schools must put appropriate security in place to safeguard personal data from unauthorised processing and accidental loss, destruction or damage.

- The Protection of Freedoms Act 2012 also requires that:
  - Schools and colleges **must** notify **each** parent 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.
  - 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 as part of an automated biometric recognition system. Further information regarding steps schools should take to identify, locate and inform parents are provided in the DfE Guidance referenced above.
  - The written consent of at least one parent must be obtained before the data are taken from the child and used. 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:
    a) the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
    b) no parent has consented in writing to the processing; or

c) a parent has objected in writing to such processing, even if another parent has given written consent.

- Reasonable alternative arrangements must be provided for pupils who do not wish to use automated biometric recognition systems to access services. The alternative arrangements must not disadvantage the pupil or parent in any way.