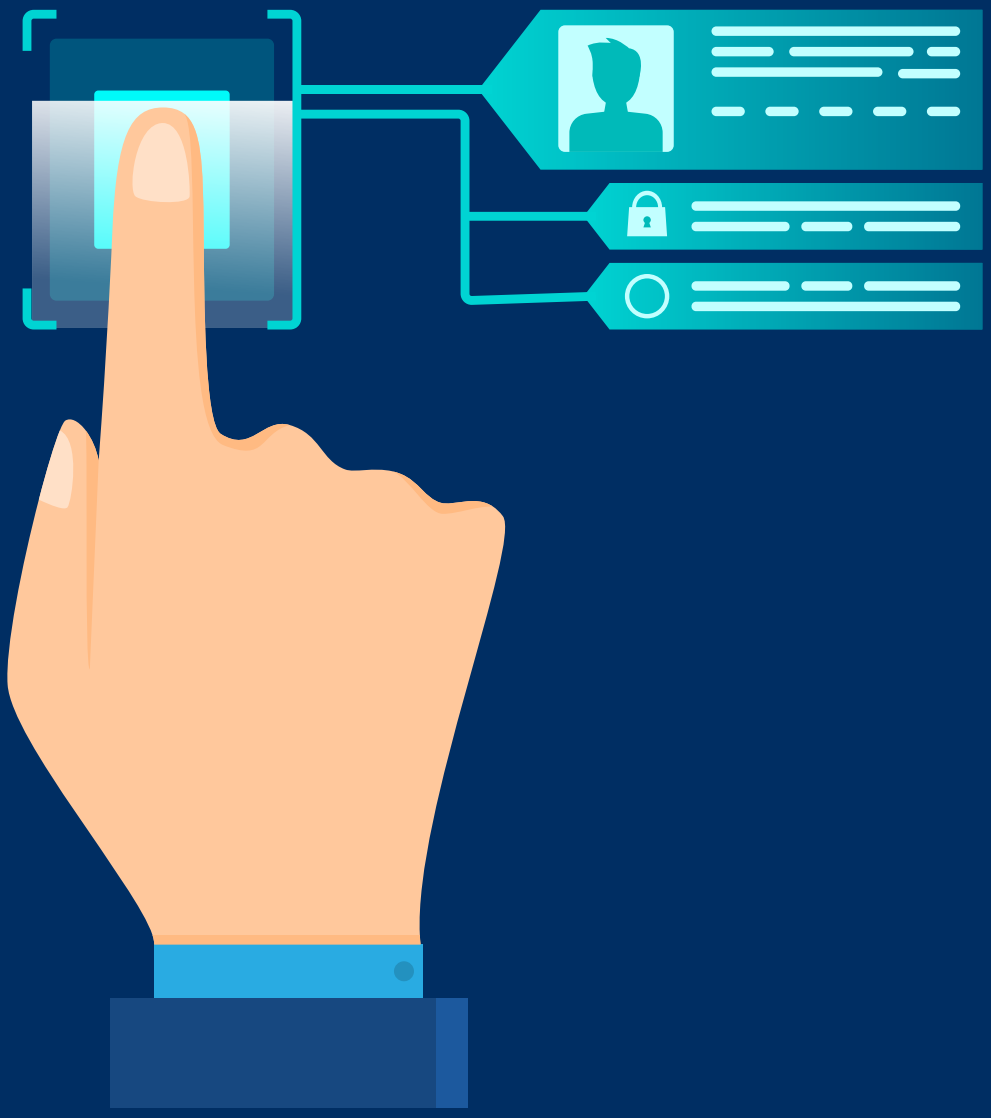
Biometrics in Schools



J A Walker, Solicitor

www.jawalker.co.uk
john@jawalker.co.uk
0333 772 9763

Biometrics in Schools

Many schools are already using biometric data, many others are actively contemplating it. The two main uses in the school setting are for attendance management and cashless catering. Some schools are currently using it as a replacement for my records, and the tracking of library books. Companies providing biometrics clearly seen other potential opportunities for schools going forwards.

However, UK GDPR and the Data Protection Act 2018 categorise biometric data as being within the most sensitive group. Even before UK GDPR came into force schools had to be mindful of the obligations in the Protection of Freedoms Act 2012.

The obligations for Maintained Schools and Academy Trusts are set out in the guidance published on 22 March 2018. This non-statutory guidance replaces the previous guidance from December 2012.

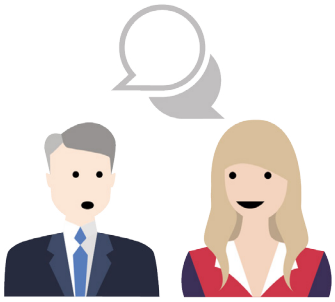
Schools and colleges using automated biometric recognition systems, or planning to install them, should make arrangements to notify parents and obtain the consent required under the duties set out in the body of this advice. There are no circumstances in which a school or college can lawfully process a pupil's biometric data without having notified each parent of a child and received the necessary consent.

Compliance is mandatory

For a school to use biometric data compliance with the obligations of the Data Protection Act 2018 and also the Protection of Freedoms Act 2012 is essential.

Use of biometric data in schools must always be with explicit consent. An alternative, which is a genuine and non-prejudicial alternative, must always be available.

Consultation and Risk Assessment



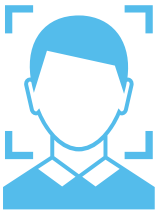
Prior to implementation of any biometric system school should be able to demonstrate genuine consultation with parents and pupils (if they are of a suitable age). This would also be required as part of a Data Privacy Impact Assessment. Any school currently using biometric recognition should review their documentation to ensure that there is evidence of the original consultation and to consider if an updated DPIA is required.

Consent

No data can be processed without the written consent of at least one parent. A record of this consent should be maintained within school.

If the pupil himself or herself objects, or if one parent consents, but the other objects, biometric processing cannot take place.

What is Biometric Data?



Biometric data could be fingerprint recognition, facial recognition, retina and iris patterns or even hand measurements.

Unsurprisingly, any technology that uses physical or behavioural characteristics is classed as a biometric recognition system.

Biometrics and UK GDPR

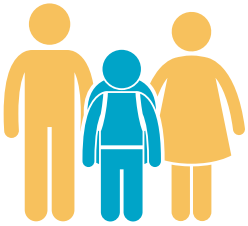
UK GDPR defined processing effectively as any interaction with data. When considering biometric processing this includes the initial recording of the data, storing the data and then using it as part of the process to identify a recognised individual. As this is processing sensitive personal data organisational safeguards must be in place.

A breach involving biometric data would be treated with grave concern by the ICO.

Information about biometric data should be contained within privacy notices.

How the security of the data is managed, retention policies and destruction mechanisms should also be set out in clear, plain language.

The importance of parental consent



When seeking to obtain consent to use biometric data the Freedom Protections Act 2012 requires schools to seek consent of parents. This may mean an absent parent, if that person is known to the school, it does not have to be the parent where the child resides.

It includes anyone who has parental responsibility, so the child is looked after by the local authority, the local authority's corporate parent must be asked to consent.

The act does of course recognise that there may be some cases where it would not be inappropriate, but in fact dangerous, to contact an absent parent. If there are safeguarding concerns of that nature be child welfare must be prioritised.

The Act establishes quite a high threshold to determining who the parents of a child are. Schools are obliged to make enquiries even if one parent does not show on the attendance register or is otherwise known to school.

What should the request for consent cover?

When notifying parents of the type of processing that the school undertakes it is important to explain:-

- **what type of biometric information has been taken**
- **how it will be used**
- **the right of the parent and pupil to object**
- **the ability to withdraw consent**
- **to expressly state the school has a duty to provide an alternative mechanism rather than biometrics**

BUT NOTE WELL

If a pupil decides they do not wish to provide biometric data, a school cannot collect or use it. The pupil's objection overrides any parental consent.

Risk management

Schools should also be mindful that given the sensitive nature of this data, there must be rigorously processes, policies and procedures in place to protect the data.

Conclusion

As biometric data is considered to be so sensitive everyone in the school community who has a responsibility for collecting, using or accessing the data needs to be aware of their own obligations to comply with relevant policies and procedures.

If at any point there is a breach and unauthorised sharing of biometric data, it must be reported as part of UK GDPR breach management as soon as an individual is aware.

Biometric data will continue to play an important part in managing aspects of school life. However ensuring that the necessary DPI assessment, ongoing risk assessments, policies and consent is in place is a rolling obligation.

An extract from the DFE guidance of the template notification and consent form is attached.