Biometric Data Policy

Formally adopted by the Governing Board of:	**Hemsby Primary School**
On:	**To be agreed Nov 2021**
Headteacher:	**Sian Harmer**
Chair of Governors:	**Kathryn Hewitt**
Review:	

Contents

Definitions

Biometric Data: Personal data resulting from specific processing relating to the physical, physiological or behavioural characteristics of a natural person, that allow or confirm the unique identification of that natural person, such as facial images.
Automated biometric recognition system: A system which measures an individual's behavioural or physical characteristics using an automated process, which compares these characteristics with biometric data in its system to confirm an individual's identity.
Processing biometric data: Any operation or set of operations which is performed on biometric data or on sets of biometric data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Special category data: Personal data containing information relating to an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, or criminal history.

Commented [1]: Personal data revealing racial or ethnic origin;political opinions; religious or philosophical beliefs; tradeunion mmebership; genetic data and biometic data for the purpose of identifying a natural person; data concerning health; and data concerning a natural persons sex life or sexual orientation.

Aims of the Policy

The Biometric Data Policy outlines the way(s) in which Hemsby Primary School uses biometric data, in line with UK GDPR, and the relevant data protection legislation, including the Data Protection Act 2018, as well as the Protection of Freedoms Act 2012.
The Biometric Data Policy works in conjunction with our Data Protection Policy and does not invalidate any of the provisions that are within these policies.

Data Protection Principles

Hemsby Primary School will uphold the principles that have been set out in The Data Protection Act 2018 and will only handle biometric data in accordance with these principles to ensure that the rights and freedoms of individuals under the relevant legislation are protected.

Hemsby Primary School will ensure that biometric data is only processed in a way that:

- Is adequate and only in a way that is necessary in relation to the purposes for which they are processed.
- Is accurate and, where reasonable, steps will be taken to correct any data that is inaccurate.
- Is processed lawfully, fairly and in a transparent manner, only collected for specific, explicit and legitimate purposes, and not in a manner that is in any way incompatible with these values.
- Ensures the security of the data and sufficiently protects the data from unauthorised access and processing. as well as protection against accidental loss, destruction or damage, using measures.
- Is retained in a manner in which identification of the data subject is permitted for no longer than is required for the purpose(s) for which the data was originally collected.

Roles and responsibilities

1. The Local Governing Authority is responsible for reviewing this policy on a bi-annual basis.
2. The Headteacher is responsible for ensuring that the provisions in this policy are upheld consistently and that the relevant individuals are aware of their roles in upholding the provisions set out in this policy.
3. The Data Protection Officer (DPO) is responsible for monitoring the school's compliance with the provisions set out in this policy in relation to biometric data and assessing when the school needs to take out a Data Protection Impact Assessment. The DPO will also act as a point of contact for the Information Commissioner's Office (ICO), as well as for individuals who are covered under this policy by having their biometric data processed by the organisation.

Data Protection Impact Assessment

A Data Protection Impact Assessment involves describing and detailing the process of collecting biometric data, from the point of collection through all stages of the data flow including its deletion at the end of the life cycle. The DPIA will also assess any risks that will

exist at any stage to the data subject's rights as well as steps that can be implemented to mitigate those risks.
The DPO will oversee any DPIA that takes place to ensure its authenticity and thoroughness.
A DPIA will take place before any biometric data is collected, or before any new process that will involve the collection of biometric data is implemented.
The potential risks associated with the proposed collection of biometric data to individuals will be of the utmost importance when a DPIA is carried out.
If the DPIA concludes that a risk exists that cannot be mitigated against, the DPO will notify the ICO of the risk, at which point the ICO will provide a written response stating whether the risk is one that is acceptable, or extra steps must be taken to minimise the risk. The ICO may also request that the organisation refrains from processing the biometric data. At all stages, we will follow the ICO's advice before processing any data.

Consent

Where the data subject(s) are under the age of 18, the relevant piece of legislation that governs the obtaining of consent with regards to biometric information is section 26 of the Protection of Freedoms Act 2012, and the school will comply with the requirements of the Act with regards to the processing of biometric data.
Before any student's biometric data is collected, the school will obtain consent from the student's parents by way of a biometric data collection form. If the school only has one of the pupil's parents' contact details on file, the headteacher will decide whether steps should be taken to obtain the contact details of the other parent in order to seek their consent.
The school is not required to seek the consent of a particular parent if the parent if:

- the parent cannot be found;
- it is in the best interests of the student that the parent isn't contacted;
- the parent is unable to give consent or withdraw consent with a sound mind; or,
- if it is not reasonably practicable or appropriate for the school to notify them.

If neither parent can be contacted to obtain consent for the processing of biometric data, the school will seek to obtain consent from the individual(s) who are responsible for the care of the pupil.

When consent is sought from a parent and/or other appropriate individuals, the school will notify them of:

- the types of biometric data that the school wishes to collect;
- how it will be collected;
- the purposes for which it will be collected;
- the data subject's right to consent and withdraw consent at any point; and,
- the alternative and reasonable arrangements that the school will put in place should consent not be obtained/withdrawn in the future.

No biometric data from a pupil under the age of 18 will be processed if:

- the pupil objects to the processing of their biometric data (whether that be in the form of verbal or non-verbal communication)
- no parent or guardian has consented to the processing of the pupil's biometric data
- or where one parent has objected (even if the other parent has consented).

Commented [2]: Before any student's biometric data is collected, the school will notify each parent of a studentthat they wish to take and subsequently use the child's biometicc data. As long as the child or a parent does not object, the written consent of only one parent will be reqired 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. Notification and Consent from the student's parents can be sought and dicumented by way of a biometric data collection form. If the school only has one of the pupil's parents' contact details on file, the headteacher will decide whether steps should be taken to obtain the contact details of the other parent in order to seek their consent.

Commented [3]: the parent lacks mental capacity to object or consent

the welfare of the child requires that a particular parent is not contacted

where it is otherwise not reasonably practicable for a particular parent to be notified or for his or her consent to be obtained.

Commented [4]: Where neither of the parents of a child can be notified and consent sought for one of the reasons as set out above then the school should notifiy and seek consent from the Local authority, if the child is looked after or is accomodated or maintained by a voluntary organisation. If the child is not looked after, accommodate or maintained by a voluntary organisation then notification should be sent to all thos caring for the child and written consent obtained from at lest one carer before the data is processed (subject to the child and none of the carers objeting)

Commented [5]: Maybe put 'prior to consent being sought ' to make it absolutely clear to the user of the docment that notification comes before consent. I think most schools are likely to se a form similar to the one in the DoE guidance to deal with notification and therafter consent.

The school will also obtain consent from staff before processing their biometric data. Parents and guardians, staff and pupils are permitted to withdraw their consent at any point, and any biometric data that the school has collected up to that point will be deleted. Alternative arrangements will be put in place for individuals who have either been unwilling to provide consent or who have withdrawn their consent for their biometric data to be processed by the school.

Alternative Arrangements

If an individual has refrained from giving their consent or has withdrawn their consent from the processing of their biometric data, the school will provide alternative arrangements that are suitable, so that the relevant service may continue to be used. Any alternative arrangements that are put in place will be such that the individual isn't put at a disadvantage, or make the accessing of the relevant service any harder.

Breaches

The school has policies in place for the protection of data subjects and the data that the school holds on them. In the event of a breach to our biometric data system will be dealt with in accordance with our Data Breach Procedure.

Data Retention

Data will be retained no longer than necessary (as documented in the organisation's record of processing, or retention schedule) or until consent is withdrawn, at which point to the data will be deleted.

Reviewing the policy

This policy will be reviewed annually by the local governing board, and the next scheduled date for renewal is stated at the beginning of this policy document.
Any changes to this policy will be communicated to pupils, parents and staff.