



**Alma
Primary**
עולם חסד יבנה
A world built on kindness

Alma Primary Protection of Biometric Data Policy

Responsibility: *Marc Shoffren*
GB Body responsible: *Main Governing Body*
Start date: *November 2024*
Review date: *Autumn 2026*

Contents

1. Statement of intent	1
2. Legal framework	1
3. Definitions.....	1
4. Roles and responsibilities	2
5. Data protection principles	2
6. Data protection impact assessments (DPIAs)	3
7. Notification and consent.....	4
8. Alternative arrangements	5
9. Storage and data retention.....	6
10. Security and breaches.....	6
11. Monitoring and review.....	6

Alma Primary **Protection of Biometric Data Policy**

1. Statement of intent

Alma Primary is committed to protecting the personal data of all its children and staff; including any biometric data we collect and process.

We collect and process biometric data in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected. We aim to treat the data collected with appropriate care, and ensure the processing is necessary and proportionate.

This policy outlines the procedure the school follows in collecting and processing biometric data.

2. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Protection of Freedoms Act 2012
- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- DfE (2022) 'Protection of biometric information of children in schools and colleges'
- DfE (2023) 'Data protection in schools'

This policy operates in conjunction with all relevant school policies.

3. Definitions

"Biometric data" is personal information about an individual's physical or behavioural characteristics, resulting from specific technical processing, which can be used to identify that person. Such data includes an individual's fingerprints, facial shape, retina and iris patterns, hand measurements, and voice. All biometric data is personal data.

An **"automated biometric recognition system"** is a system which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically', i.e. electronically. Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual. Biometric recognition systems can use many kinds of physical or behavioural characteristics, such as those listed above.

"Processing biometric data" includes obtaining, recording or holding the data or carrying out any operation on the data including disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

Alma Primary **Protection of Biometric Data Policy**

- Recording biometric data for children or adults, e.g. taking measurements from a fingerprint via a fingerprint scanner.
- Storing biometric information on a database for children or for adults.
- Using biometric data as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise children or adults.

“**Special category data**” is personal data which the UK GDPR says is more sensitive, and so needs more protection. Where biometric data is used for identification purposes, e.g. through keystroke analysis, it is considered special category data.

4. Roles and responsibilities

The Governing Body will be responsible for:

- Ensuring data protection performance is monitored regularly.
- Providing support to the DPO, as necessary.
- Ensuring effective network security infrastructure is in place to keep personal data protected.

The headteacher will be responsible for:

- Ensuring the provisions in this policy are implemented consistently.
- Ensuring relevant staff receive appropriate training on data protection as deemed necessary.
- Deciding on how the school processes and uses biometric data.

The DPO will be responsible for:

- Monitoring the school’s compliance with data protection legislation in relation to the use of biometric data.
- Identifying the additional risks associated with using automated biometric technology by conducting a data protection impact assessment (DPIA).
- Being the first point of contact for the ICO and for individuals whose data is processed by the school and connected third parties.

5. Data protection principles

The school will process all personal data, including biometric data, in accordance with the key principles set out in the UK’s GDPR. The school will ensure biometric data is:

- Processed lawfully, fairly and in a transparent/carer manner.
- Only collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.

Alma Primary Protection of Biometric Data Policy

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date, and that reasonable steps are taken to ensure inaccurate information is rectified or erased.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

As the data controller, the school will be responsible for being able to demonstrate its compliance with the provisions outlined above.

Where relevant, information will be included in the school's privacy notices explaining how biometric data is to be processed and stored, including the rights available to individuals in respect of the processing.

6. Data protection impact assessments (DPIAs)

Prior to implementing a system that involves processing biometric data and/or processing biometric data, a DPIA will be carried out. The DPO will oversee and monitor the process of carrying out the DPIA.

The DPIA will:

- Describe the nature, scope, context and purposes of the processing.
- Assess necessity, proportionality and compliance measures.
- Identify and assess risks to individuals.
- Identify any additional measures to mitigate those risks.
- Be reviewed frequently and kept updated.

When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered. If a high risk is identified that cannot be mitigated, the DPO will, where possible, consult the ICO before the processing of the biometric data begins.

The ICO will provide the school with a written response (within eight weeks or 14 weeks in complex cases) advising whether the risks are acceptable, or whether the school needs to take further action. In some cases, the ICO may advise the school to not carry out the processing. The school will adhere to any advice from the ICO, unless the Governing Body considers it necessary not to do so.

Each DPIA will be treated as a 'living' document to help manage and review the risks of the processing of the biometric data and the measures put in place on an ongoing basis. DPIAs will be reviewed annually or in response to any changes.

7. Notification and consent

Consent requirements for biometric information are imposed by section 26 of the Protection of Freedoms Act 2012.

Where the school uses children's biometric data as part of an automated biometric recognition system (e.g. using fingerprints to receive school dinners instead of paying with cash), the school will comply with the requirements of the Protection of Freedoms Act 2012.

Prior to any biometric recognition system being put in place or processing children's biometric data, the school will send relevant parents/carers a Biometric Data Notification and Consent Form. Digital consent will be sought from at least one parent/carer of the child before the school collects or uses a child's biometric data.

The name and contact details of parents/carer will be taken from the school's MIS (Management Information System). Where the name of only one parent/carer is recorded, the headteacher will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent/carer.

The school does not need to notify a particular parent/carer or seek their consent if the Headteacher is satisfied that:

- The parent/carer cannot be found, e.g. their whereabouts or identity is not known.
- The parent/carer lacks the mental capacity to object or consent.
- The welfare of the child requires that a particular parent/carer is not contacted.
- It is otherwise not reasonably practicable for a particular parent/carer to be notified or for their consent to be obtained.

Where neither parent/carer of a child can be notified for any of the reasons set out above, consent will be sought from the following individuals or agencies as appropriate:

- If a child is being 'looked after' by the LA or is accommodated or maintained by a voluntary organisation, the LA or voluntary organisation will be notified and their written consent obtained.
- If the above does not apply, then notification will be sent to all those caring for the child and written consent will be obtained from at least one carer before the child's biometric data is processed.

Notification sent to parents/carers and other appropriate individuals or agencies will include information regarding the following:

- Details about the type of biometric information to be taken
- How the data will be used
- How the data will be stored

Alma Primary Protection of Biometric Data Policy

- The parent's/carer's and the child's right to refuse or withdraw their consent
- The school's duty to provide reasonable alternative arrangements for any child whose information cannot be processed

The school will not process the biometric data of a child under the age of 18 in the following circumstances:

- The child (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data
- No parent/carer or carer has consented in writing to the processing
- A parent/carer or carer has objected in writing to such processing, even if another adult has given written consent

Parents/carers and children will be made aware that they can object to participation in the school's biometric systems or withdraw their consent at any time, and that if they do this, the school will provide them with an alternative method of accessing the relevant services. The steps taken by the school to inform children will take account of their age and level of understanding. Parents/carers will also be informed of their child's right to object and will be encouraged to discuss this with their child.

Where a child or their parents/carers object, any biometric data relating to the child that has already been captured will be deleted. If a child objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the school will ensure that the child's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the child's parent.

Where staff members or other adults use the school's biometric systems, consent will be obtained from them before they use the system. Staff and other adults can object to taking part in the school's biometric systems and can withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted.

Where staff or volunteers utilise school devices which have biometric security devices, such as fingerprint recognition technology (i.e. iPads or laptops), and the adult chooses to use the biometric device, they will be deemed to have met the consent requirements of this policy and no further validation or recording of their permission will be required.

Alternative arrangements will be provided to any individual that does not consent to take part in the school's biometric systems, in line with the section of this policy below.

8. Alternative arrangements

Parents/carers, children, staff members and other relevant adults have the right to not take part in the school's biometric systems.

Alma Primary Protection of Biometric Data Policy

Where an individual objects to taking part in the school's biometric systems, reasonable alternative arrangements will be provided that allow the individual to access the relevant service, e.g. where a biometric system uses a child's fingerprints to pay for school meals, the child will be able to use an alternative payment method for the transaction instead, which will not put the individual at any disadvantage or result in any additional burden being placed on the individual or the child's parents/carers, where relevant.

9. Storage and data retention

Biometric data will be managed and retained in line with the relevant school policies. The school will only store and process biometric information for the purpose for which it was originally obtained and consent provides.

If an individual, including a child's parent, where relevant, withdraws their consent for their or their child's biometric data to be processed, the school will take steps to ensure that any biometric data which has been saved is erased from the school's system in an appropriate time frame, normally within 6 weeks.

10. Security and breaches

Biometric data will not be unlawfully disclosed to third parties. The outcome of the DPIA will be used to identify the security measures that will be put in place to protect any unlawful and/or unauthorised access to the biometric data stored by the school. These security measures and the process that will be followed if there is a breach to the school's biometric systems are detailed in the school's Cyber-security Policy and other relevant policies.

11. Monitoring and review

The governing board will review this policy at least every two years, or earlier in the event there is a serious breach of the policy.

Any significant changes made to this policy will be communicated to all staff, parents/carers and children, as relevant.