LILY LANE
PRIMARY SCHOOL

Kenyon Lane, Moston, M40 9JP
0161 205 3397

Biometric Data Policy

This policy was agreed by the Governing Body in September 2022 and supersedes all previous policies relating to this area.	
Signed by Chair of Governors:	
Implemented:	**September 2022**
Review Date:	**September 2023**
Author:	**M. Hussain-Ahmed**

www.lilylane.manchester.sch.uk

Introduction

Lily Lane Primary School (herein referred to as the school) is committed to protecting the personal data of its staff; this includes any biometric data processed.

In order to safeguard the personal data processed on school systems, access to certain devices is protected with fingerprint and facial recognition technology. This helps to ensure that staff do not share passwords and adds an extra layer of protection in the event a device is lost or stolen. Devices include school owned mobile phones and tablets that staff use to communicate and access systems.

The school collects and processes any biometric data in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected. This policy outlines the procedure the school follows when collecting and processing biometric data.

Objectives

This policy aims to ensure that:

- The processing of biometric data is fully complaint with the relevant legislation and guidance.
- Any potential data breaches are prevented as much as reasonably practicable.
- Individuals are informed and confident the school are handling their biometric data securely.
- To ensure staff and key departments understand and adhere to the processes set out in this policy.

Scope

This policy applies to all staff employed by the school. The school currently only process biometric data relating to staff; no pupil biometric data is processed.

Legal Framework

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

- Protection of Freedoms Act 2012
- Data Protection Act 2018
- UK General Data Protection Regulation (UK-GDPR)
- Department for Education (DfE) (2018) Protection of biometric information of children in schools and colleges

This policy operates in conjunction with the following school policies:

- Data Protection Policy
- Retention/Records Management Policy
- Data Breach Policy & Procedure
- Online Safety & Acceptable Use Policies

Key Definitions

Biometric data: Personal information about an individual's physical or behavioural characteristics that can be used to identify that person, including their fingerprints, facial shape, retina and iris patterns, and hand measurements.

Automated biometric recognition system: 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 to identify that individual.

Processing biometric data: 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 example would include using a fingerprint to gain entry to a device or system.

Special category data: Personal data which the UK-GDPR says is more sensitive, and so needs more protection – where biometric data is used for identification purposes, it is considered special category data.

Roles & Responsibilities

The school governing board is responsible for reviewing this policy on an annual basis.

The Headteacher is responsible for ensuring the provisions in this policy are implemented consistently and making sure that adequate resources are in place to fulfil the requirements set out in this policy.

The Data Protection Officer (DPO) is responsible for monitoring the school's compliance with data protection legislation in relation to the use of biometric data.

Data Protection Principles

The school processes all personal data, including biometric data, in accordance with the key principles set out in the UK-GDPR.

The school ensures biometric data is:

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

The school is the Data Controller for personal data processed and is responsible for complying with the provisions outlined above.

Data Protection Impact Assessments (DPIA's)

Prior to processing biometric data or implementing a system that involves 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.

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 consult the ICO before any processing of that data begins.

The ICO will provide the school with a written response within 8weeks (or 14weeks for 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.

Notification & Consent

The school will ensure that staff are informed that biometric data is being processed via the use of this policy and the Staff Privacy Notice. In addition, the school understand that there is an obligation to obtain consent for the processing of biometric data.

Staff will be issued with a consent form (appendix a) that clearly outlines what data is being processed and why; an option to withdraw consent and instructions to do so will be provided. Consent is reviewed for staff on an annual basis for the relevant data processing activities.

Any staff member that does not consent to the use of biometric data will be provided with an alternative means of accessing the relevant school systems. This will likely be via the use of a password. Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant system; nor will it result in any additional burden being placed on the individual.

Should a staff member withdraw consent at any point, the school will securely delete any biometric information that has been captured up until that point in time and offer an alternative method of access.

To ensure the protection of biometric data, the school will only select providers that share the school's commitment to protecting personal information.

Retention of Biometric Data

The school will ensure all biometric data is processed in accordance with its Records Management Policy & Retention Schedule.

As a rule of thumb, biometric data will be removed as soon as a staff members employment ends with the school as part of the process to remove access to systems. Biometric data will typically be associated with an Apple ID / Google ID which is used to access the school system via a device such as phone / tablet; access will be removed, and all login credentials deleted prior to the device being reissued to another staff member.

The school will remove and delete any data sooner should the staff member withdraw consent.

A log of all devices and access arrangements is kept as part of the school's asset register and permissions process.

Breaches

The school ensure appropriate control and technical security measures as much as possible but understand that on occasion, although rarely gaps can occur that can potentially lead to a data breach. The school ask that all staff review and agree to the following policies to prevent data breaches:

- Acceptable Use Policy for Staff
- Cyber Security Policy

To summarise, the school ask that staff:

- Lock away any devices when not in use
- Inform the relevant IT lead or update the asset register to track any devices removed from the school premises
- Be mindful not to leave devices unattended within or outside of school and report immediately to the DPO if any devices are lost / stolen.
- Inform the IT lead should they wish to remove biometric entry to their device so that alternative arrangements can be made.

In the event that a data breach occurs, a full policy and procedure is in place to instruct staff how to report and mitigate any negative impacts.

Monitoring & Review

This policy will be reviewed on an annual basis or sooner should a change in legislation or procedure occur. The school will review this policy and associated documentation accordingly should a new biometric data processing activity take place or be amended.

Appendix 1 – Biometric Data – Consent Form

Please refer to the school's policy on biometric data prior to reviewing and signing this consent form.

The school would like to ask your permission to use your biometric data in order to provide you with secure access to the devices that we provide you with as part of your employment. Most school owned devices such as mobile phones, tablets and some laptops have built in capabilities to set up secure access using:

- Your fingerprint
- Facial recognition

Biometric data is a secure and efficient method of logging into your school owned device(s) as it allows for quick login, prevents the need to remember or write down passcodes and adds an extra layer of security if devices happen to get lost or stolen.

Once set up, your device will automatically recognise your fingerprint or facial profile (dependent upon device) that is has scanned and stored at the point of setup. The device will allow automatic entry each time your biometric data is scanned.

It will be your choice as the user to decide whether you would like to set up the use of fingerprint or facial recognition entry to devices issued to you; the school is however required to keep a log of your login preferences and any back up passcodes should the device be compromised. Biometric data for this purpose will be associated with the device ID and stored securely in the cloud until removed by the school.

Please note that the use of biometric data is optional; alternative passcode entry will be provided for those that opt out. In addition, you can remove your consent at any time if you change your mind by contacting the School Business Manager (SBM).

Please tell us whether you would like us to set up biometric access to your device:

Would you like to use biometric data?	**Tick:**
Yes: I would like to use biometric data to access school systems via the device(s) issued to me.	
No: Please provide alternative arrangements as I do not wish to use biometric data to access school systems via the device(s) issues to me.	

Please review and confirm that you have understood the following:

- I have read and understood the school's biometric data policy
- I have read and understood what biometric data will be processed, why and how it is stored
- I understand that the use of biometric data is optional, and I can withdraw my consent at any time by contacting the SBM

- I understand how my biometric data will be stored and that it will be securely deleted if I withdraw consent or leave my role at school
- I understand the school will keep a log of back up passcodes to gain entry to my school owned devices
- I have read and understood the school's cyber security and acceptable use policies.

I confirm that I have read and understood the terms above:

Print Name	
Signature:	
Date:	

Please return this form to the school office at your earliest convenience.