St Augustine's Academy

General Data Protection Regulation (GDPR) and Biometric Information Policy

Approved by:		**Date:**	22.10.25
Next review due by:	September 2026		

'Let your light shine before others, that they may see your good deeds and glorify your Father in Heaven."

Matthew 5:16

General Data Protection Regulation (GDPR) and Biometric Information Policy

Introduction

The General Data Protection Regulation (GDPR) is a piece of EU-wide legislation which will determine how people's personal data is processed and kept safe, and the legal rights individuals have in relation to their own data.

'Personal data' means information that can identify a living individual.

The regulation continues to apply to all schools from 25 May 2018, even after the UK leaving the EU. The regulation has been adopted into UK law and is now referred to as UK GDPR. All references to GDPR or UK GDPR in this document should be taken to refer to UK GDPR

The statutory requirement for all schools to have a policy for the 'Protection of Biometric Information' came into force from September 2019. See DfE (2018) 'Protection of biometric information of children in schools and colleges'

Definitions of Biometric Testing are as follows:

- 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 in order to recognise or identify the 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 automated biometric recognition system processes data when:

    Recording pupils' biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.

    Storing pupils' biometric information on a database.

    Using pupils' biometric data as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise pupils.

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

Legal framework

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

- The Data (Use and Access) Act 2025
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA)
- School Standards and Framework Act 1998
- Freedom of Information Act 2000
- Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- Protection of Freedoms Act 2012

This policy also has regard to the following guidance:

- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2012) 'IT asset disposal for organisations'
- DfE (2018) 'Data protection: a toolkit for schools'
- DfE (2025) 'Dealing with subject access requests (SARs)
- ICO (2025) What should we consider when responding to a request?

Rationale

The School collects and uses personal information about staff, students, parents or carers and other individuals who come into contact with the School. This Policy sets out the manner in which personal data is processed fairly and lawfully.

Personal information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the School complies with its statutory obligations.

The School is a data controller and must therefore comply with the Data Protection Principles in the processing of personal data, including the way in which the data is obtained, stored, used, disclosed and destroyed. The School must be able to demonstrate compliance. Failure to comply with the Principles exposes the School and staff to civil and criminal claims and possible financial penalties.

Details of the School's purpose for holding and processing data can be viewed on the data protection register: https://ico.org.uk/esdwebpages/search

The Schools registration number is **Z3294759**. This registration is automatically renewed annually and renewed on **2nd October 2025**.

Please note, in some instances due to statutory regulations, this policy does not apply e.g. staff grievances, allegations of abuse.

At St Augustine's Academy, we do not collect, store or use any type of biometric information and therefore the remainder of this policy refers only to GDPR. If this changes in the future, then a separate 'Protection of Biometric Information Policy' will be put in place.

Statement of Intent

St. Augustine's Academy aims to:

- Process personal data in compliance with the General Data Protection Regulations
- Ensure that staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities under this policy
- Safeguard the data protection rights of those involved with the school community
- Instil confidence in the school's ability to process data in a fair and secure way

Scope

This Policy applies to the following:

- Personal data of all School employees, governors, students, parents and carers, volunteers and any other person carrying out activities on behalf of the School.
- The processing of personal data, both in manual form and on computer.
- All staff and governors.

Data Protection Principles

The GDPR sets out the key principles that all personal data must be processed in line with. St. Augustine's Academy will thereby ensure that personal data will be the following:

- Processed fairly, lawfully and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

- Processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

There are also stronger rights for individuals regarding their own data. These rights are as follows:

- To be informed about what data is held, why it is being processed and who it is shared with
- To access their data
- To rectification of the record
- To erasure
- To restrict processing
- To data portability
- To object to processing
- To not to be subject to automated decision-making including profiling

Roles and Responsibilities

The Governing Body and the Headteacher are responsible for implementing good data protection practices and procedures within the school and for the compliance with the Data Protection Principles.

It is the responsibility of all staff to ensure that their working practices comply with the Data Protection Principles. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures forming part of this policy.

The requirements of this policy are also mandatory for any third party contracted to provide services to the school.

The Data Protection Officer will have responsibility for all issues relating to the processing of personal data and will report directly to the Headteacher. The Data Protection Officer will comply with responsibilities under the GDPR and will deal with subject access requests for rectification and erasure, and data security breaches. All complaints about data processing will be dealt with in accordance with the School's Complaints Policy.

The school's Data Protection Officer is Julia Holloway.

Strategies

- Staff will receive training on the data protection requirements with specific relation to school policy
- GDPR protocols and practice will form part of the induction process for new staff
- Privacy Notices for staff and stakeholders will be transparent. They will be written in a form easily understandable by those determined as 'Children' under the ICO legislation. Privacy notices advise whose personal data is

held, the purposes for which data is processed and who it will be shared with. https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-noticestransparency-and-control/

- The GDPR Policy and Privacy Notices will be available on the school's website

Consent

Where the school seeks consent for processing personal data, such as the use of photographs, it will ensure that appropriate signed consent is obtained. Consent forms will detail how consent can be withdrawn. For all children under the age of 16, written consent will be required from the adult with parental responsibility.

Location of personal information and data

Hard copy data, records, and personal information are stored out of sight and in locked cupboards when not in use or unattended.

The only exception to this is medical information that may require visibility or immediate access during the school day and is necessary for the well-being of the person involved.

Sharing data with third parties and data processing on behalf of the School

Personal data will only be shared with appropriate authorities and third parties where it is fair and lawful to do so e.g. local authorities, Ofsted or the Department of Health. Any sharing will be undertaken by trained personnel using secure methods. Where a third party undertakes data processing on behalf of the School e.g. by providing cloud based systems or shredding services, the School will ensure that there is a written agreement requiring the data to be processed in accordance with the Data Protection Principles.

Data may be shared with the following:

- Examination Authorities – To register pupils for examinations/tests and enable them to sit for them
- Education Establishments – Data will be shared to allow a smooth transition for pupils moving to another school
- Health Authorities - As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.
- Police and courts - If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.
- Social workers and support agencies - In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

- Educational division - Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education

Subject Access Requests

Requests for access to personal data (Subject Access Requests)(SARs) will be processed by the Data Protection Officer. Those making a Subject Access Request will be charged a fee in accordance with Regulations. Records of all requests will be maintained.

The School will comply with the statutory time limits for effecting disclosure in response to a Subject Access Request. The statutory time period is one calendar month of receipt of the request.

Data Protection Breaches

Breaches of personal or sensitive data will be notified within 72 hours to the individual(s) concerned and the ICO.

Disposal of personal data

Paper documentation containing personal information that is no longer required will be shredded. Paper based documents containing personal information will never be placed in recycling bins

Any disposal of IT assets holding data shall be in compliance with ICO guidance and in collaboration with the school's IT support. Demonstrable competence in providing secure disposal would be sought for any companies contracted to deal with the disposal of secure information from St. Augustine's Academy, https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf

Guidelines for staff:

- All passwords used to access computers, memory sticks or systems where personal data is stored must use a mixture of lower case letters, upper case letters, symbols and numbers in their passwords
- School computers should be locked or shut down when unattended and at the end of the school day
- Only transport electronic information from school on a secure computing device i.e. password protected laptops and memory sticks
- Use pseudonyms and anonymise personal data where possible
- Ensure that all postal and e-mail addresses are checked to ensure safe dispatch of information. When sending personal information by post the envelope should clearly state 'Private – Contents for Addressee only.'
- Avoid taking paper based documentation out of school wherever possible. If paper-based documentation is taken out of school then please ensure that it is kept secure e.g. lockable drawer at home or in a sealed envelope which

indicates a return address if misplaced. Return it to school as soon as possible.

- When transporting paper based documentation, make sure that it is locked during transit e.g. in the locked boot of a car. Never leave documentation in vehicles overnight
- Lock documentation containing personal information away at night and when not being used during the daytime e.g. Pupil Provision Maps
- Shred documentation containing personal information and never put paper based documents containing personal information into recycling bins
- Collect paper copies of printouts containing personal information from printers/photocopies immediately
- Avoid e-mailing documents to personal e-mail addresses
- Never store work related documents on a shared home computer and never let school computers/laptops be used by others e.g. sons/daughter's homework use
- Only print off documents containing personal data if absolutely necessary
- Report any loss of paper-based information or portable computer devices to the Data Protection Officer/Headteacher immediately
- Personal passwords, where the accessing of personal data is possible, must not be shared with others. Passwords of staff leaving the school should be changed/removed in a timely manner
- The personal details of others, at social events or in public places, must not be discussed. Take care if reading documentation containing personal information on public transport or leaving personal information unattended in a public place e.g. meeting, course
- Only copy necessary recipients into e-mail correspondence and only post necessary information when sending information via the postal service
- Always ask the Data Protection Officer/Headteacher if you are unsure about storage/transportation or sharing of information containing personal information

Monitoring and Review

This policy shall be monitored for changes to the applicable regulations and reviewed on an annual basis.