

‘Love your neighbour as yourself.’ There is no commandment greater than this.

Mark 12: Verse 31



Data Protection Policy

Author:	VP Teaching, Learning & Assessment
Date adopted by Governors/Academy:	September 2017
Date of last review/amendment:	February 2019
Date of next review:	September 2020

‘Love your neighbour as yourself.’ There is no commandment greater than this.

Mark 12: Verse 31

Introduction

At All Saints Academy our vision is “Living Well Together with **Dignity, Faith and Hope**”. We aspire to take dignified decisions and afford dignity to all members of our community, regardless of background or circumstance. Our position as a Voluntary Aided Church Academy means that the Christian faith has a central role in all of our actions and decisions. We strive for excellence in all that we do, enabling our students to transform their lives and to hope for happy and successful futures.

Our vision translates into our everyday practice. The values of **Dignity, Faith and Hope** are particularly relevant in ensuring all in our community are encouraged to strive for excellence through service to others. This policy exists to provide a framework for supporting our stated aim of “*Living Well Together with Dignity, Faith and Hope*”, and this translates into our everyday practice. **Living Well Together** includes ensuring the welfare of young people, and through the general ethos of the academy, we will seek to persuade students in need of support to come forward. This will be promoted through the PSHCE curriculum, assemblies and tutor time.

Our vision translates into our everyday practice. The values of **Dignity, Faith and Hope** are particularly relevant in ensuring ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

To function properly the academy needs to collect and use certain types of information about staff, students and other individuals who come into contact with the academy. We are also obliged to collect and use data to fulfil our obligations to the LA, DfE and other bodies. This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this in the General Data Protection Regulation introduced on 25th May 2018.

We regard the lawful and correct treatment of personal information as very important to successful operations, and to maintaining confidence between those with whom we deal and ourselves. We ensure that our organisation treats personal information lawfully and correctly.

Purpose

As we strive for excellence we must also engender trust that the organisation adheres to policy. This policy is intended to ensure that we adhere to the Principles of Data Protection, as detailed in the General Data Protection Regulation.

The principles of the General Data Protection Regulation

So far as is reasonably practicable, the Trust’s organisations will comply with the principles of Article 5 of the GDPR to ensure all data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

‘Love your neighbour as yourself.’ There is no commandment greater than this.

Mark 12: Verse 31

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- processed in a manner 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.

Article 5 (2) requires that:

- “the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

Processing Personal Data

The Trust’s organisations undertake to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects’ right of access. This is included in the Privacy Notice given to data subjects.

We collect and process pupil information under Article 6 and Article 9 of the General Data Protection Regulation from 25 May 2018. Under Article 6(1)(e) our lawful basis for processing data is that it is a Public task and the processing is necessary for us to perform a task in the public interest. Under Article 9(2)(g) our lawful basis for processing sensitive data is that processing is necessary for reasons of substantial public interest. We also collect and use data under section 537A of the Education Act 1996 and section 83 of the Children’s Act 1989.

We collect and process staff data under Article 6 and Article 9 of the General Data Protection Regulation from 25 May 2018. Under Article 6(1)(e) our lawful basis for processing data is that it is a Public task and the processing is necessary for us to perform a task in the public interest. Under Article 9(2)(g) our lawful basis for processing sensitive data is that processing is necessary for reasons of substantial public interest. We also collect your data in line with section 114 of the Education Act 2005.

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

‘Love your neighbour as yourself.’ There is no commandment greater than this.

Mark 12: Verse 31

The rights that relate to our data subjects will be included in our Privacy Notice that is given out to the data subjects.

Organisation

Within the academy we will, through appropriate management, apply strict application of criteria and controls:

- observe fully conditions regarding the fair collection and use of information
- meet its legal obligations to specify the purposes for which information is used
- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- ensure the quality of information used
- apply strict checks to determine the length of time information is held
- ensure that the rights of people about whom information is held, can be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken, the right of access to one’s personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information). See Appendix 1
- take appropriate technical and organisational security measures to safeguard personal information
- ensure that personal information is not transferred abroad
- treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- set out clear procedures for responding to requests for information

We will also ensure that:

- there is someone with specific responsibility for Data Protection within the academy (Data Manager)
- everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice
- everyone managing and handling personal information is appropriately trained to do so
- everyone managing and handling personal information is appropriately supervised
- anybody wanting to make enquiries about handling personal information knows what to do
- queries about handling personal information are promptly and courteously dealt with
- methods of handling personal information are clearly described
- a regular review and audit is made of the way personal information is held, managed and used
- methods of handling personal information are regularly assessed and evaluated
- performance with handling personal information is regularly assessed and evaluated
- a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against the members of staff concerned

Rights of Access

The GDPR extends to all data subjects the right of access to their own personal data. Where a request for subject access is received from a student, the Trust’s policy is that:

- Requests from students will be processed as a subject access request as outlined below and a copy of the information will be given directly to the student, unless it is clear that the student does not understand the nature of the request.

‘Love your neighbour as yourself.’ There is no commandment greater than this.

Mark 12: Verse 31

- Requests from students who do not appear to understand the nature of the request will be referred to their parents.
- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

Processing Subject Access Requests

Requests for access must be made in writing to the Data Controller, and responses will be made as soon as is practicably possible and in accordance with legally-prescribed timescales. This is no more than a month from the date of the request however the trust will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, we will inform the individual within one month of the receipt of the request and explain why the extension is necessary. Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of the request will be deemed to be the date on which sufficient information has been provided. The contact details are provided on the Privacy Notices.

The Trust may take legal advice in determining what information may be released. Certain data is exempt from the right of access under the GDPR, and this may include:

- Information that identifies other individuals,
- Information that the School or College reasonably believes is likely to cause damage or distress,
- Information that is subject to legal professional privilege,
- Student test scripts.

Unless otherwise stated, the Trust’s organisations will treat as confidential any reference they give.

The Trust acknowledges that an individual may have the right to access a reference relating to them which is received by the Academy. Such references will only be disclosed if such disclosure does not identify the source of the reference, or if the referee has given their consent, or if disclosure is reasonable in the particular circumstances.

Exemptions

Certain data is exempted from the provisions of the GDPR. Information relating to the following will not be released to individuals:

- The prevention or detection of crime;
- The assessment of any tax or duty;
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the Trust.

The above are examples only of some of the exemptions under the Regulation. Parents and students should note that any information relating to child protection, or which reveals the identity of another student, will not be released.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the Trust can:

‘Love your neighbour as yourself.’ There is no commandment greater than this.

Mark 12: Verse 31

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

Where the trust refuses to respond to a request, we will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Retention

The Academy Trust will retain your data for a set period of time. The data will be stored securely and, once the retention period has lapsed, secure disposal methods will be implemented.

Refer to Appendix A for detailed information regarding data retention.

Data Controller and Data Protection Officer

The Academy Trust is the Data Controller. It determines the purposes and means of processing data in line with the General Data Protection Regulation. The trust will also appoint a Data Protection Officer as it is a public body. The DPO will assist the trust in monitoring internal compliance, inform and advise on our data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Obligation for data processor to notify data controller

- The data processor will notify the data controller without undue delay after becoming aware of the breach.

Obligation for data controller to notify the supervisory authority

- The data controller will notify the supervisory authority under GDPR if it's likely to result in a risk to people's rights and freedoms. This decision should be taken in consultation with the Executive Principal and the Data Protection Officer.

‘Love your neighbour as yourself.’ There is no commandment greater than this.

Mark 12: Verse 31

There is no requirement to notify if unlikely to result in a risk to the rights and freedoms of natural persons (Article 33, clause 1)

- Notification to the ICO to be made without undue delay and not later than 72 hours.
- Description of the nature of the breach
 - Categories of data
 - Approximate numbers of records and data subjects affected
- Describe likely consequences
- Describe measures taken – or to be taken – to mitigate the breach
- Communicate details of the Data Protection Officer
- If the trust fails to report within 72 hours this must be explained to the ICO
- The Trust must document personal data breaches, effects and remedial action. This will enable assessment of compliance with these requirements.

Obligation for data controller to communicate a personal data breach to data subjects

- The trust must communicate to the data subject without undue delay if a high risk. The decision to communicate should be taken in consultation with the Executive Principal and the Data Protection Officer.
- Communication will be in clear plain language
- The supervisory authority may compel communication with data subject
- Exemptions if:
 - appropriate technical and organisational measures taken
 - high risk to data subject will not materialise
 - communication with data subject would involve disproportionate effort

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the General Data Protection Regulation.

‘Love your neighbour as yourself.’ There is no commandment greater than this.

Mark 12: Verse 31

APPENDIX A

Data Retention

Governing Body

Basic description	Statutory Provisions (if applicable)	Retention Period	Action at the end of the retention period
Agendas for Governing Body meetings		One copy should be retained	