Data Protection Policy

FROM OCTOBER 2023

Aquinas Church of England Education Trust

Policy control			
Title	Data Protection		
Responsibility	Data Protection Lead		
Review body	Trust Board		
Suite	Data Protection		
Approval date	October 2023		
Review date	October 2025		
Version	V2		
Version	**Date**	**Author**	**Note of revisions**
V2	01/10/23	MCA	General Updates

Data Protection

Overview

Statement of Intent

AQUINAS Church of England Education Trust (the Trust) acknowledges that it is necessary to collect and use certain types of personal data about staff, pupils, parents, volunteers, trustees, and other individuals who encounter the Trust and its academies, and to use data to fulfil obligations to stakeholders, the Department for Education, local authority, and other bodies. The Trust and its academies will deal with all information properly in whatever way it is collected, recorded, and used – on paper, biometric, electronic/digital, or recorded on other material. The Trust regards the lawful and correct treatment of personal data as very important to successful operations and to maintaining confidence between its stakeholders, those with whom it deals with and to itself. We will ensure that personal data is dealt with lawfully and correctly and organisational methods for keeping data secure are in place supported by clear practical policies and written procedures. To this end, the Trust fully endorses and adheres to the principles of data protection, as detailed in the UK General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA) collectively referred to as the Legislation.

[UPDATED] This policy is in place to ensure all staff and those involved in the governance of the Trust are aware of their responsibilities and outlines how the Trust complies with the core principles of the Legislation.

References to staff or pupils at an academy shall include all employees undertaking services in relation to an academy nursery, being a provision to provide care and education for children between the ages of 2 years and 4 years, where appropriate. References to Headteacher includes executive Headteacher and head of school as relevant.

This policy does not form part of any employee's contract of employment, and it may be amended at any time. Any breach of this policy by employees will be taken seriously and may result in disciplinary action and serious breaches may result in dismissal. Breach of the Legislation may expose the Trust to enforcement action by the Information Commissioner's Office (ICO), including fines. Furthermore, certain breaches can give rise to personal criminal liability for the Trust's employees. At the very least, a breach of the Legislation could damage our reputation and have serious consequences for the Trust and for our stakeholders.

1. Legal framework

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

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

This policy also has regard to the following guidance:

- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- DfE (2018) 'Data protection: a toolkit for schools'
- ICO (2012) 'IT asset disposal for organisations'

[NEW] This policy is integral to the Trust's operations where such operations necessitate the processing of personal data. It is also applicable to all Trust and academy policies which necessitate the processing of personal data. These policies are detailed in appendices 1 and 2 of the Trust's Policy Overview document.

[NEW] In particular, this policy should be read in conjunction with the Trust's:

- CCTV Policy

- Freedom of Information Act Policy
- IT Policy
- Management and Retention of Records Policy
- Photography Policy
- Safeguarding and Child Protection Policy

2. Data protection principles

Personal Data

Personal data is defined as data which relates to a living individual who can be identified directly or indirectly from that data or other information held. The Legislation applies to both automated personal data and to manual filing systems.

- Special category personal data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, the processing of genetic or biometric data for the purposes of uniquely identifying a person, data concerning health or data concerning a natural person's sex life or sexual orientation. It does not include data about criminal allegations, proceedings, or convictions. In the case of criminal offence data, schools are only able to process this if it is either:
    - Under the control of official authority; or
    - Authorised by domestic law. The latter point can only be used if the conditions of the reason for storing and requiring the data fall is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health, and research.

The Lawful Basis for Processing Personal Data

The Trust processes data, including biometric data, in accordance with data protection principles. All members of staff employed by the Trust are required to adhere to the six data protection principles set out in the Legislation:

1. Personal data is processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. The personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
4. The personal data is accurate and, where necessary, kept up to date and reasonable steps are taken to ensure that inaccurate personal information is erased or rectified.
5. Personal data is kept in a form which permits identification of the individual (data subjects) for no longer than is necessary for the purposes for which the personal data is processed.

6. Personal data is 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.

Processing Personal Data

Processing is defined in the Legislation as collecting, recording, or holding the information or data. It also covers the carrying out of any operation on the data to include:

- Organisation, structuring, storage adaptation or alteration.
- Retrieval, consultation, or use.
- Disclosure by transmission, dissemination or otherwise making available.
- Alignment or combination, restriction, erasure, or destruction.

[NEW] The legal basis for processing data will be identified and documented prior to data being processed. Under the Legislation, personal data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for a contract held with the individual, or because they have asked the school to take specific steps before entering a contract.
- Processing is necessary for compliance with a legal obligation (not including contractual obligations).
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Processing is necessary for protecting vital interests of a data subject or another person, i.e., to protect someone's life.
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights, or freedoms of the data subject – this condition is not available to processing undertaken by the Trust or its academies in the performance of its tasks.

[NEW] The school will only process personal data without consent where any of the above purposes cannot reasonably be achieved by other, less intrusive means or by processing less data.

[UPDATED] Special Category Personal Data

The Trust will be processing special category personal data about our stakeholders. We recognise that the law states that this type of data needs more protection. We must therefore be more careful with the way in which we process special category personal data.

When special category personal data is being processed, as well as establishing a lawful basis for processing the personal data, a separate condition for processing it must be met. In most cases the relevant conditions are likely to be that:

- The Data Subject's explicit consent to the processing of such data has been obtained.

- Processing is necessary for reasons of substantial public interest, based on Union or Member State law which shall be proportionate to the aim pursued, where we respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.
- Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the Data Subject in the field of employment law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject.

The Trust recognises that in addition to special category personal data, we are also likely to process information about our stakeholders which is confidential in nature, for example, information about family circumstances, child protection or safeguarding issues. Appropriate safeguards must be implemented for such information, even if it does not meet the legal definition of special category personal data.

3. Trust practice

The Trust, as data controller in most cases, will operate through appropriate management and the strict application of criteria and controls to:

- Ensure that personal data is processed in compliance with the processing conditions detailed in the GDPR.
- Notify the ICO that we process personal data and when procedures change or are amended.
- Notify the ICO of a personal data breach within 72 hours of us becoming aware of a breach unless a breach is unlikely to cause a risk to the rights and freedoms of data subjects.
- Observe fully the conditions regarding the lawful, fair, and transparent collection and use of personal data. To achieve this, we have in place and use privacy notices.
- Meet legal obligations to specify the purposes for which personal data is processed.
- Collect and process appropriate personal data, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Maintain internal records of the categories of personal data processed and the lawful basis for the processing.
- Ensure the quality of personal data used and shared.
- Not keep personal data for longer than is necessary for the purposes for which it is processed.
- Ensure that the rights of people about whom personal data is held, can be fully exercised under the Legislation. (These include: the right to be informed why personal data is being collected and how it is being processed; the right of access to

an individual's personal data; the right to rectification where it is inaccurate or incomplete; the right to erasure in certain specified circumstances; the right to restrict or object to processing in certain circumstances; the right to data portability.)

- All recruitment and vetting checks (including Disclosure and Barring Services records) are kept in a safe central place and are kept in accordance with safeguarding protocols.
- Take appropriate technical and organisational security measures to safeguard personal data.
- Ensure that personal data is not transferred abroad without suitable safeguards.
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation, or ethnicity when dealing with requests for personal data.
- Set out clear procedures for responding to requests for personal data.
- Secure methods for safely disposing of all electronic and paper records.
- Ensure photographs of students at the academies are not included in any Trust or academy publication or website without specific consent.
- Ensure that where CCTV captures or processes images of identifiable individuals it is done so in line with data protection principles.
- Ensure that there are appropriate technical and organisational measures to demonstrate that personal data is processed in line with the principles set out in the Legislation.

The Trust will also ensure that:

- There is someone with specific responsibility for data protection within the Trust and at each academy.
- Everyone managing and handling personal data understands that they are responsible for following good data protection practice.
- Everyone managing and handling personal data is appropriately trained to do so.
- Everyone managing and handling personal data is appropriately supervised.
- Queries about handling personal data are promptly and courteously dealt with.
- Methods of handling personal data are clearly described.
- A regular review and audit are made of the way personal data is held, managed, and used.
- A breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against the members of staff concerned.
- When information is authorised for disposal, it is done appropriately.

Criminal Convictions and Offences

There are separate safeguards in the Legislation for personal data relating to criminal convictions and offences.

It is likely that the Trust and its academies will process personal data about criminal convictions or offences. This may be because of pre-vetting checks we are required to undertake on staff, Aquinas advisory council members and trustees or due to information which we may acquire during their employment or appointment.

In addition, from time to time we may acquire information about criminal convictions or offences involving pupils or parents. This information is not routinely collected and is only likely to be processed by the Trust in specific circumstances, for example, if a child protection issue arises or if a parent / carer is involved in a criminal matter.

Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and / or the Police. Such information will only be processed to the extent that it is lawful to do so, and appropriate measures will be taken to keep the personal data secure.

This policy will be updated as necessary to reflect best practice or amendments made to the Legislation and guidance from the ICO.

4. Responsibility

Trustees are ultimately responsible for data protection and implementing the appropriate technical and organisational measures to demonstrate that personal data is processed in accordance with the legislation. The day-to-day management of complying with this responsibility has been delegated to the Chief Executive Officer (CEO). The Trust has also appointed a Trust Data Protection Officer (Trust DPO) as required by the Legislation.

Trust DPO	Contact Details
Mary Capon	Write to: AQUINAS Trust Magpie Hall Lane BROMLEY BR2 8HZ. Tel No: 020 3949 7000 Email: info@aquinastrust.org

The Trust DPO is responsible for:

- Informing and advising the organisation and its employees of their obligations to comply with the Legislation.
- To monitor compliance with the Legislation such as managing internal data protection activities, advising on data protection impact assessments, training staff, and conducting internal audits.
- First point of contact for supervisory authorities and for individuals whose personal data is being processed.
- The DPO should be involved, in a timely manner, in all issues relating to the protection of personal data. To do this, the Legislation requires that DPOs are provided with the necessary support and resources to enable the DPO to effectively carry out their tasks. Factors that should be considered include the following:
    - senior management support.
    - time for DPOs to fulfil their duties.
    - adequate financial resources, infrastructure (premises, facilities, and equipment) and staff where appropriate.

- official communication of the designation of the DPO to make known existence and function within the organisation.
- access to other services, such as HR, IT, and security, who should provide support to the DPO.
- continuous training so that DPOs can stay up to date regarding data protection developments.
- where a DPO team is deemed necessary, a clear infrastructure detailing roles and responsibilities of each team member.
- whether the Trust should give the DPO access to external legal advice to advise the DPO on their responsibilities under this Data Protection Policy.

- The DPO is responsible for ensuring that the Trust's processing operations adequately safeguard personal data, in line with legal requirements. This means that the governance structure within the Trust must ensure the independence of the DPO.
- The Trust will ensure that the DPO does not receive instructions in respect of the carrying out of their tasks, which means that the DPO must not be instructed how to deal with a matter, such as how to investigate a complaint or what result should be achieved. Further, the DPO should report directly to the highest management level, i.e., the board of directors.
- The requirement that the DPO reports directly to the trustees ensures that trustees are made aware of pertinent data protection issues. If the Trust decides to take a certain course of action despite the DPO's advice to the contrary, the DPO should be given the opportunity to make their dissenting opinion clear to the board and to any other decision makers.
- A DPO appointed internally by the Trust is permitted to undertake other tasks and duties for the organisation, but these must not result in a conflict of interests with his or her role as DPO. It follows that any conflict of interests between the individual's role as DPO and other roles the individual may have within the organisation impinge on the DPO's ability to remain independent.
- To avoid conflicts the DPO cannot hold another position within the organisation that involves determining the purposes and means of processing personal data. Senior management positions such as chief executive, chief financial officer, head of marketing, head of IT or head of human resources positions are likely to cause conflicts. Some other positions may involve determining the purposes and means of processing, which will rule them out as feasible roles for DPOs.
- In the light of this, the Trust will take the following action to avoid conflicts of interests:
    - draw up internal rules to this effect to avoid conflicts of interests which may include, for example, allocating some of the DPO's other duties to other members of staff, appointing a deputy DPO and / or obtaining advice from an external advisor if appropriate.
    - include a more general explanation of conflicts of interests.

- declare that the DPO has no conflict of interests regarding his or her function as a DPO, as a way of raising awareness of this requirement.
- include safeguards in the internal rules of the organisation and ensure that the job specification for the position of DPO or the service contract is sufficiently precise and detailed to avoid conflicts of interest.

[UPDATED] The responsibility for data protection at each academy has been delegated by trustees to the Headteacher of the academy. To assist Headteachers with the discharge of these responsibilities, academy data protection leads (academy DPL) have been appointed for each academy as follows:

Academy	Data Protection Lead	Contact Details
Bishop Justus CE School	Juliana Poloczanska	sbm@bishopjustus.bromley.sch.uk
Cudham CE Primary School	TBC, until such time please contact the Trust's DPO	
Keston CE Primary School	Jennifer Davall	admin@keston.bromley.sch.uk
Parish CE Primary School	Charlotte Davey	admin@parish.bromley.sch.uk
Rye College	TBC, until such time please contact the Trust's DPO	
Rye Community Primary School	TBC, until such time please contact the Trust's DPO	
St. George's CE Primary School	Anne Browne	admin@st-georgesbickley.bromley.sch.uk
St. John's CE Primary School	Nicola Stilwell	admin@st-johns.bromley.sch.uk
St. Mark's CE Primary School	Pietra Salmasi	admin@st-marks.bromley.sch.uk
St. Nicholas CE Primary School	Karen Crawford	admin@chislehurst-cofe.bromley.sch.uk
Trinity CE Primary School	Elizabeth Smith	info@trinityceprimary.school

The Headteacher and academy DPL will be responsible for:

- Implementing this policy and ensuring that staff at the academy are aware of their data protection responsibilities.
- Monitoring and auditing academy data protection activities.
- Being the first point of contact for dealing with requests from individuals whose personal data is being processed by the academy and where appropriate actioning the request in accordance with the Trust data protection procedures.
- Alerting the CEO and Trust DPO where there has been a security breach in relation to personal data held at the academy.

5. [UPDATED] Individual rights

1. An individual has the right to be informed about why personal data is being collected and how it will be processed. A privacy notice must be provided at the time the data is collected which complies with the individual's rights as detailed in the Legislation. Where the service is offered directly to a pupil, the privacy notice will be in clear and plain language to ensure that the pupil can understand it. Where it is not possible to provide the privacy notice at the time the data is collected, it will be provided as soon as is reasonably possible.

However, the Trust wishes to adopt a layered approach to keeping people informed about how we process their personal data. This means that the privacy notice is just one of the tools we will use to communicate this information. Trust employees are expected to use other appropriate and proportionate methods to tell individuals how their personal data is being processed if personal data is being processed in a way that is not envisaged by our privacy notices and / or at the point when individuals are asked to provide their personal data, for example, where personal data is collected about visitors to academy premises or if we ask people to complete forms requiring them to provide their personal data.

[NEW] The privacy notice will include the following information:

- The identity and contact details of the controller, the controller's representative, where applicable, and the DPO.
- The nature of the personal data being processed and why.
- The purpose of, and the lawful basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to withdraw consent at any time and lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

[NEW] Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided – this information will be supplied at the time the data is obtained.

[NEW] Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided – this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

2. **[UPDATED]** Individuals have a right to access their personal data, once their identity has been verified, within 1 calendar month of the request. Such a request, termed a subject access request (SAR), must be responded to within 1 month free of charge; however, the Trust or an academy may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual

requests further copies of the same information. Where a request is manifestly unfounded, excessive, or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information. The period for complying with the request can be extended to 2 further months where the request is complex. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within 1 month of the receipt of the request.

[NEW] Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

[NEW] Where a SAR has been made for information held about a child, the Trust will evaluate whether the child is capable of fully understanding their rights. If the Trust determines the child can understand their rights, it will respond directly to the child.

[NEW] Where a request is manifestly unfounded or excessive, the Trust holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within 1 month of the refusal.

[NEW] The Trust will ensure that information released in response to a request does not disclose personal data of another individual. If responding to the request in the usual way would disclose such data, the Trust will:

- Omit certain elements from the response if another individual's personal data would be disclosed otherwise.
- Reject requests that cannot be fulfilled without disclosing another individual's personal data unless the individual consents or it is reasonable to comply without consent.
- Explain to the individual who made the request why their request could not be responded to in full.

[NEW] In the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify the information the request is in relation to – the time limit for responding to the request will be paused until clarification from the individual is received.

[NEW] The individual has a right of complaint to the ICO where they are not satisfied with the Trust's response to their request.

3. **[UPDATED]** Where the information is inaccurate or incomplete, the individual has the right to request rectification. Where the information has been disclosed to a third party, rectification of personal data will also be advised to the third party. The request for rectification must be responded to within 1 month, this period may be extended by 2 months where the request is complex, but the individual will be kept informed. Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, the Trust may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once. The Trust reserves the right to refuse to process

requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

[UPDATED] The Trust will take reasonable steps to ensure that data is accurate or is rectified if inaccurate, implementing a proportional response for data that has a significant impact on the individual, e.g., if significant decisions are made using that data. The Trust will restrict processing of the data in question whilst its accuracy is being verified, where possible.

Where no action is being taken in response to a request for rectification, or where the request has been investigated and the data has been found to be accurate, the Trust will explain the reason for this to the individual. The individual has a right of complaint to the ICO where the request for rectification is not actioned.

4. **[UPDATED]** An individual may request the deletion or removal of their personal data where there is no compelling reason for its continued processing. Individuals, including children, have the right to erasure in the following circumstances:
    i. The personal data is no longer necessary in relation to the purpose for which it was originally obtained.
    ii. Consent for its use is withdrawn.
    iii. The personal data was unlawfully processed.
    iv. The individual objects to the processing and there are no overriding legitimate interests for continuing the processing.
    v. The personal data must be erased to comply with a legal obligation.
    vi. The personal data is processed in relation to the offer of information society services to a child.

    The Trust may refuse to do so because the personal data is necessary to comply with a legal obligation, public interest task, exercise of official authority or defence of legal claims.

    Where the processing of personal data causes damage or distress to the individual, especially a pupil, the Trust will give greater weight to such a request.

    As a pupil may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a pupil has given consent to processing and later requests erasure of the data, regardless of age at the time of the request.

    [NEW] The Trust has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

    - To exercise the right of freedom of expression and information
    - To comply with a legal obligation for the performance of a public interest task or exercise of official authority
    - For public health purposes in the public interest
    - For archiving purposes in the public interest, scientific research, historical research, or statistical purposes

- The establishment, exercise, or defence of legal claims

[NEW] The Trust has the right to refuse a request for erasure for special category data where processing is necessary for:

- Public health purposes in the public interest, e.g., protecting against serious cross-border threats to health.
- Purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services.

[NEW] Requests for erasure will be handled free of charge; however, the Trust may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

[NEW] Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so. Where personal data has been made public within an online environment, the Trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

5. [UPDATED] The Trust will inform individuals, including children, of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information. Individuals, including children, have the right to object to the following:
    - Processing based on legitimate interests or the performance of a task in the public interest
    - Processing used for direct marketing purposes
    - Processing for purposes of scientific or historical research and statistics.

    [NEW] Where personal data is processed for the performance of a legal task or legitimate interests:

    - An individual's grounds for objecting must relate to his or her situation.
    - The Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise, or defence of legal claims, or, where the Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the individual.
    - The Trust will respond to objections proportionally, granting more weight to an individual's objection if the processing of their data is causing them substantial damage or distress.

    [NEW] Where personal data is processed for direct marketing purposes:

    - The right to object is absolute and the Trust will stop processing personal data for direct marketing purposes as soon as an objection is received.

- The Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

[NEW] The Trust will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future.

[NEW] Where personal data is processed for research purposes:

- The individual must have grounds relating to their situation to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the Trust is not required to comply with an objection to the processing of the data.

[NEW] Where the processing activity is outlined above, but is carried out online, the Trust will offer a method for individuals to object online.

[NEW] The DPO will ensure that details are recorded for all objections received, including those made by telephone or in person, and will clarify each objection with the individual making the request to avoid later disputes or misunderstandings. The Trust will respond to all objections without undue delay and within 1 month of receiving the objection; this may be extended by a further 2 months if the request is complex or repetitive.

[NEW] Where no action is being taken in response to an objection, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the ICO and to a judicial remedy.

6. **[UPDATED]** Individuals can restrict the use of the personal data by the Trust where:
    - The accuracy or use of the information is contested, and the Trust has yet to decide. Use can also be restricted where processing is unlawful or no longer necessary, but the personal data is being retained for legal reasons.
    - Where an individual has objected to the processing and the Trust is considering whether their legitimate grounds override those of the individual.
    - Where processing is unlawful, and the individual opposes erasure and requests restriction instead.
    - Where the Trust no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim.

[NEW] If processing is restricted, the Trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future. The Trust will inform individuals when a restriction on processing has been lifted.

[NEW] Where the Trust is restricting the processing of personal data in response to a request, it will make that data inaccessible to others, where possible, e.g., by

temporarily moving the data to another processing system or unpublishing published data from a website.

[NEW] If the personal data in question has been disclosed to third parties, the Trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

[NEW] The Trust reserves the right to refuse requests for restricting processing if they are manifestly unfounded or excessive or if exemptions apply. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within 1 month of the refusal.

7. **[NEW]** Individuals, including children, have the right to obtain and reuse their personal data for their own purposes across different services. The right to data portability only applies in the following cases:
    - Where personal data has been provided directly by an individual to a controller.
    - Where the processing is based on the individual's consent or for the performance of a contract.
    - When processing is carried out by automated means.

    [NEW] Personal data can be easily moved, copied, or transferred from one ICT environment to another in a safe and secure manner, without hindrance to usability. Personal data will be provided in a structured, commonly used, and machine-readable form. Where feasible, data will be transmitted directly to another organisation at the request of the individual. The Trust will not be required to adopt or maintain processing systems which are technically compatible with other organisations.

    [NEW] The Trust will provide the information free of charge.

    [NEW] If the personal data concerns more than one individual, the Trust will consider whether providing the information would prejudice the rights of any other individual.

    [NEW] The Trust will respond to any requests for portability within 1 month. Where the request is complex, or several requests have been received, the timeframe can be extended by 2 months, ensuring that the individual is informed of the extension and the reasoning behind it within 1 month of the receipt of the request.

    [NEW] Where no action is being taken in response to a request, the Trust will, without delay and at the latest within 1 month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

Consent to Processing by an Individual

[UPDATED] In some circumstances, the Trust may rely on consent as the lawful basis for processing personal data. Consent will not always be needed as often another lawful basis for processing personal data will apply. An individual must consent by virtue of a positive, clear, specific affirmation to processing. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes. Consent will only be accepted where it is

freely given, specific, informed and an unambiguous indication of the individual's wishes. Consent can be withdrawn by the individual at any time.

[UPDATED] Where a pupil is under the age of 13, the consent of parents, guardians or those that hold parental responsibility will be sought prior to the processing of their data except where the processing is related to preventative or counselling services offered directly to children. Where consent is not is not provided in accordance with the requirements of the Legislation another lawful basis for processing the personal data applies. If we require consent for processing personal data about pupils aged 13 or over, we will require the consent of the pupil although, depending on the circumstances, academies should consider whether it is appropriate to inform parents / carers about this process. Consent is likely to be required if, for example, an academy wishes to use a photo of a pupil on its website or on social media. Consent is also required before any pupils are signed up to online learning platforms. Such consent must be from the parent if the pupil is aged under 13. When relying on consent, we will make sure that the child understands what they are consenting to, and we will not exploit any imbalance in power in the relationship between us. However, an appropriate age of consent is considered by the academies on a case-by-case basis, considering the requirements outlined above. A record of the consents provided will be maintained by the Trust and its academies.

The consents relied upon prior to the implementation of the GDPR will be reviewed. Where they are not GDPR compliant, they will be refreshed in accordance with the requirements of the GDPR.

Subject Access Request (SAR Procedure)

Any individual who makes a request for access to the personal data we are processing about them is making the request under the Legislation.

Requests from parents in respect of their own child will be processed as requests made on behalf of the Data Subject (the child) where the pupil is aged under 13 (subject to any exemptions that apply under the Act or other legislation). Where a parent or carer makes a request for access to the personal data held on their child, it may be necessary to obtain the consent of the child prior to the request being complied with if the child is aged 13 or over if there is no other lawful basis for sharing the personal data with the parent (subject to any enactment or guidance which permits the Trust to disclose the personal data to a parent without the child's consent). If consent is not given to disclosure, the Trust shall not disclose the personal data if to do so would breach any of the data protection principles. If there is a court order in place which relates to information regarding any pupil, that order must, regardless of other circumstances, be observed.

It should be noted that the Education (Pupil Information) (England) Regulations 2005 do not apply to academies so the rights available to parents in those Regulations to access their child's educational records are not applicable to academies in the Trust. Instead, requests from parents for personal data about their child must be dealt with under the GDPR (as outlined above). This is without prejudice to the obligation on the Trust in the Education (Independent School Standards) Regulations 2014 to provide an annual report of each

registered pupil's progress and attainment in the main subject areas taught to every parent (unless they agree otherwise in writing).

Dealing with a request for personal data

The following procedures will be followed in relation to a request for personal data:

1. A request must be made in writing (which includes the use of email). Following receipt of any written request for personal data, the member of staff must forward it to the Trust DPO, the academy Headteacher and academy DPL (where the request is received at academy level). Reasonable adjustments will be made in relation to requests from individuals who suffer from a disability as defined in the Equality Act 2010.
2. If the Trust or the academy cannot identify the information required from the initial request, it will be referred to the requester for clarification.
3. The CEO and the Headteacher must be confident of the identity of the individual making the request; consequently, the requester may be asked to provide evidence of identity. Where the request concerns the personal data of a child, this evidence will be required in addition to proof of relationship with the child.
4. An individual only has the automatic right to access information about themselves. Requests from family members, carers or parents of a minor will be considered. The CEO or Headteacher will have responsibility for ensuring the child's welfare is appropriately considered in deciding whether to comply with a request. In the event of a child having sufficient capacity to understand (normally age 13 or above) the Headteacher should ask the pupil for their consent. There may be circumstances in which a child can refuse their consent to a request.
5. The response time in relation to a request by an individual for their personal data is 1 calendar month from the date of the request or where clarification or verification of identity is requested by the Trust or academy, from the date that clarification or verification of identity is provided. Where the request is complex or involves a large volume of information, the period can be extended by 2 months, but the requester will be advised where this is the case.
6. All files will be reviewed before any disclosure takes place. Under no circumstance will access be granted immediately or before this review process has taken place. This will ensure that only personal data of the requester is disclosed, and the Trust and academy's safeguarding responsibilities are complied with. The Trust will consider whether any exemptions apply to the personal data that is requested. If so, the exempt information must be properly redacted.
7. Where information has been provided to the Trust or an academy by a third party, for example by the Local Authority, the police, a health care professional, or another school, but is held by the Trust or an academy it will be usual to seek the consent of the third party before disclosing information. This must be done early in the process to stay within the 1-month timescale. Even if the third party does not consent, or consent is explicitly not given, the data may be disclosed if it is reasonable in all the circumstances to do so. In these cases, it may be appropriate to seek additional advice of the Trust DPO.
8. The requester will be provided with the following:

- Details of the personal data that the Trust or academy holds.
- Copy of the personal data.
- Purpose(s) for which the personal data is processed.
- Recipients and third parties with whom the personal data is shared.
- If data has been withheld, the requester will be given an explanation as to why and details of who to contact in the event of a complaint.

Please see the ICO website (https://ico.org.uk/) for independent guidance.

9. Any personal data that could cause serious harm to the physical, emotional, or mental health of a pupil or another person may not be disclosed, nor should information that would reveal that the child is at risk of abuse. The same stricture applies to information relating to court proceedings.
10. Where all the data in a document cannot be disclosed, the data will be obscured from the document, or it will be retyped if appropriate. In any event a copy of the full document (before obscuring) and the altered document will be retained together with the reason why the document was altered (for audit trail purposes). If there are concerns about the disclosure of information, then additional advice will be sought.
11. Information can be provided by post (registered mail) or using electronic means. The Trust / Academy should take steps to ensure that the personal data is shared securely. Any codes, technical terms or abbreviations will be explained. Any data which is difficult to read or illegible will be retyped.
12. The Legislation applies only to living individuals.

6. Management of personal data

The Trust and academies maintain personal data in accordance with the principles detailed in the Legislation and the practices detailed above.

The Trust and academies are aware of the categories of information processed and ensure that the personal data processed is necessary for the processing activity and complies with the conditions for processing as detailed in the Legislation.

Personal data is retained for as long as is necessary to satisfy the purpose for which it is collected or to comply with a legal obligation. Retention periods for personal and other data is detailed in the Trust's document management and retention policy.

Personal data processed by the Trust and its academies in a paper format is held securely within the relevant Trust site.

Personal data processed by the Trust and its academies in a digital format is held securely in accordance with the Trust's IT policy.

7. [NEW] Automated decision making and profiling

[NEW] The Trust will only ever conduct solely automated decision making with legal or similarly significant effects is the decision is:

- Necessary for entering or performance of a contract.

- Authorised by law.
- Based on the individual's explicit consent.

[NEW] Automated decisions will not concern a child nor use special category personal data, unless:

- The Trust has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest.

[NEW] The Trust will conduct a DPIA for automated decision making to mitigate risk of errors, bias, and discrimination.

[NEW] The Trust will ensure that individuals concerned are given specific information about the processing and an opportunity to challenge or request a review of the decision.

[NEW] Individuals have the right not to be subject to a decision when both of the following conditions are met:

- It is based on automated processing, e.g., profiling
- It produces a legal effect or a similarly significant effect on the individual

[NEW] The Trust will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

[NEW] When automatically processing personal data for profiling purposes, the Trust will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

8. Privacy by design and data protection impact assessments

The Trust will act in accordance with the Legislation by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how it has considered and integrated data protection into processing activities. Staff will be trained accordingly.

[NEW] The Trust will implement a data protection by design and default approach by using several methods, including, but not limited to:

- Considering data protection issues as part of the design and implementation of systems, services, and practices.
- Making data protection an essential component of the core functionality of processing systems and services.
- Automatically protecting personal data in ICT systems.

- Implementing basic technical measures within the networks and ICT systems to ensure data is kept secure.
- Promoting the identity of the DPO as a point of contact.
- Ensuring that documents are written in plain language so individuals can easily understand what is being done with personal data.

Where appropriate data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy. DPIAs will allow the Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals. The Legislation obliges us to conduct DPIAs in respect to high-risk processing.

We will also undertake a DPIA as a matter of good practice to help us to assess and mitigate the risks to pupils. If our processing is likely to result in a high risk to the rights and freedom of children, then a DPIA should be undertaken.

A DPIA must include:

- A description of the processing, its purposes and the Trust's legitimate interests if appropriate.
- An assessment of the necessity and proportionality of the processing in relation to its purpose.
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

9. Data security

1. The Trust has taken steps to ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data Subjects may apply to the courts for compensation if they have suffered damage from such a loss.
2. The Legislation requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.
3. We will develop, implement, and maintain safeguards appropriate to our size, scope, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.
4. Members of staff and trustees ("Data Users") are responsible for protecting the personal data we hold. Data Users must implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Data Users must exercise particular care

in protecting special category personal data from loss and unauthorised access, use or disclosure.

5. Data Users must follow all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction. Data Users must comply with all applicable aspects of data security as detailed in this policy and the Trust's IT policy and procedures and not attempt to circumvent the administrative, physical, and technical safeguards we implement and maintain in accordance with the Legislation and relevant standards to protect personal data.
6. Data Users must be aware that it is a criminal offence for someone to knowingly or recklessly obtain or disclose personal data without the Trust's consent (or to ask someone to do it on their behalf) and / or to retain it without our knowledge (for example, if a member of staff accesses personal data about pupils or other members of staff without our consent and / or shares that data with people who are not permitted to see it). It is also an offence to sell or try to sell such personal data. These offences will also be treated as disciplinary issues in accordance with the Trust's HR policies.
7. It is the responsibility of all Data Users to work together to ensure that the personal data we hold is kept secure. We rely on our colleagues to identify and report any practices that do not meet these standards so that we can take steps to address any weaknesses in our systems. Anyone who has any comments or concerns about security should notify the Headteacher of the relevant academy or the Trust DPO.
8. <u>Paper records</u>
    - Personal data held in hard copy format will be kept in a locked filing cabinet, drawer, safe or similar to mitigate the risk of theft, damage, or destruction.
    - Personal data held in hard copy format will be kept in locked filing cabinets to avoid unauthorised access. Staff should not remove personal data out of the Trust or academies. A clear desk policy is advisable in relation to personal data to avoid unauthorised access, theft, or loss.
    - The Trust site must be locked securely to avoid unauthorised access, theft, and loss. The security arrangements and procedures must be detailed in the academy's health and safety or premises management procedures.
    - Personal data removed from a Trust site for whatever reasons must be always kept secure. It should not be left where it is at risk of theft or destruction. Personal data removed from a Trust site should not be left unattended; where it is unattended it should be held securely in a locked room or premises.
    - The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
9. <u>Digital records</u>
    - All work electronic devices and access to servers are password-protected to safeguard against unauthorised access.
    - Ensure that the server environment (where relevant) is kept clean and managed to prevent access by unauthorised personnel.

- Digital personal data is coded, encrypted or password-protected and is saved on a network drive that is regularly backed up off-site, where possible.
- Work laptops and PCs should primarily be used for work related matters.
- Staff are provided with their own secure login and password, which is regularly changed, to access the IT network.
- Work PCs and laptops should be locked or shut down to prevent unauthorised use when the user is away from their desk.
- Wherever possible, ensure that personal data is not stored on the hard drive of any work laptop, PC, or mobile storage device including memory sticks, phones, tablet device or CDs.
- Where personal data is saved on removable storage or a portable device, the device such as a memory stick, it should be encrypted, the data password protected and the device kept in a locked filing cabinet, drawer or safe when not in use.
- Work related personal data should not be downloaded onto a personal PC or laptop.
- Where possible, electronic devices are enabled to allow the remote blocking or deletion of data in case of theft.
- Emails containing sensitive or confidential information are password-protected (with the recommended number of characters) especially if there are unsecure servers between the sender and the recipient.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- **[UPDATED]** Documents must be scanned with encryption or password protected if they contain personal data.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security. The person taking the information from the school premises accepts full responsibility for the security of the data
- Before sharing data, all staff members will ensure:
- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.
- Ensure that there a Trust and academy business continuity plan in relation to electronically held information.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are always supervised.

The Trust's IT Policy should be reviewed further details on digital security and steps to be taken in the event of a digital breach.

10. Breach of data security

If there is a breach or suspected breach of data security within the Trust's central operations (Aquinas Central) or at an academy, the issues shall be managed as detailed below. A personal data breach (PDB) is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data whether in paper or digital format.

1. Where the PDB occurs at an academy, the member of staff must inform the Headteacher and academy DPL immediately.
2. The Aquinas Critical Incident team (Aquinas CIT) must be informed immediately by the Headteacher or academy DPL. For the purposes of a PDB, the Aquinas CIT consists of the CEO, the Trust DPO, Director of Human Resources, and the Chief Financial Officer.
3. Where the PDB occurs at Aquinas central the Aquinas CIT must be informed immediately.
4. The Aquinas CIT will:
    i. Assessing any breach of personal data security by identifying the issues and the extent of the breach as a matter of urgency.
    ii. Speak to all the parties involved in the breach.
    iii. Consider the physical and IT consequences of a breach of data security.
    iv. Take the necessary steps to limit the extent and impact of the destruction, loss, alteration, unauthorised disclosure of, or access to, personal information whether in paper or digital format by either securing the appropriate IT systems where the breach is digital or the appropriate physical precautions where the information is held manually.
    v. Secure the appropriate forensic investigation to ascertain the extent of the breach.
    vi. Agree a communication strategy to deal with the PDB.
    vii. Consider the harm caused by the breach of data security.
    viii. Report to the police if appropriate.
    ix. Keep records of the response.
    x. Notify the Information Commissioner's Office within 72 hours of the breach if appropriate.
    xi. Consider the events that resulted in the PDB and the protocol which needs to be put in place to avoid future issues.

The ICO will be notified within 72 hours of the Trust becoming aware of a breach where the breach is likely to result in a risk to the rights and freedoms of the individual and if unaddressed it is likely to have a significant effect on the individual. The notification will include the following information:

1. The nature of the personal data breach including categories and number of individuals concerns and the categories and numbers of personal data records affected.
2. Name and contact details of the DPO.

3. Description of the likely consequences of the breach; and
4. Description of the measures taken or proposed to be taken to deal with the breach and the mitigation to limit any adverse effect.

[NEW] In addition, the individuals affected by the breach must also be notified if there is likely to be a high risk to the rights and freedoms of individuals. Where notifying an individual about a breach to their personal data, the Trust will provide specific and clear advice to individuals on the steps they can take to protect themselves and their data, where possible and appropriate to do so.

[NEW] The Trust will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented.

[NEW] Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

[NEW] The Trust will work to identify the cause of the breach and assess how a recurrence can be prevented, e.g., by mandating data protection refresher training where the breach was a result of human error.

11. Publication information

The Trust's publication scheme, detailed in the Trust's Freedom of Information Policy, outlines the classes of information that will be made routinely available, including:

- Company documents
- Policies and procedures
- Annual reports
- Financial information

Classes of information specified in the publication scheme are made available quickly and easily on request.

The Trust and its academies will not publish any personal information, including photos, on its website without the permission of the affected individual unless doing so would be consistent with the data protection principles.

When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

12. Biometric data

Biometric data is 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. Biometric data is a type of special category personal data.

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 to recognise or identify the individual.

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 an individual's biometric data, e.g., taking measurements from a fingerprint via a fingerprint scanner.
- Storing an individual's biometric information on a database.
- Using an individual's 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.

Academies in the Trust may process biometric data as part of an automated biometric recognition system, for example, for cashless catering or photo ID card systems where an individual's photo is scanned automatically to provide him or her with services.

Where the Trust or an academy undertakes the processing of biometric data, a data protection impact assessment will be undertaken. 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 Trust's Data Protection Officer will consult the ICO before the processing of the biometric data begins. The ICO will provide the Trust with a written response (within eight weeks or 14 weeks in complex cases) advising whether the risks are acceptable, or whether the Trust needs to take further action. In some cases, the ICO may advise the Trust to not carry out the processing. Individuals will be informed that they can object or refuse to allow their biometric data to be collected and used via a letter.

The Trust and/or the relevant academies must obtain the explicit consent of parents of pupils, staff, and any other data subjects before processing their biometric data.

Where biometric data relating to pupils is processed, the relevant academy must ensure that each parent of a child is notified of the academy's intention to use the child's biometric data and obtain the informed, written consent of at least one parent before the data is taken from the pupil and used as part of an automated biometric recognition system. When contacting parents to obtain consent, the name and contact details of the pupil's parents will be taken from the academy's admission register. Where the name of only one parent is included on the admissions register, the Data Protection Officer will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent.

The academy does not need to notify a particular parent or seek their consent if it is satisfied that:

- The parent cannot be found, e.g., their whereabouts or identity is not known.
- The parent lacks the mental capacity to object or consent.

- The welfare of the pupil requires that a particular parent is not contacted, e.g., where a pupil has been separated from an abusive parent who must not be informed of the pupil's whereabouts.
- It is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.

Where neither parent of a pupil can be notified, consent will be sought from the following individuals or agencies as appropriate:

- If a pupil 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 pupil and written consent will be obtained from at least one carer before the pupil's biometric data can be processed.

Notification sent to parents 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.
- The parent's and the pupil's right to refuse or withdraw their consent.
- The academy's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed.

An academy must not process the biometric data of a pupil under 18 years of age where:

- the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data; in activities that involve the processing of their biometric data, the academy will ensure that the pupil's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the pupil's parent(s).
- no parent has consented in writing to the processing; or
- a parent has objected in writing to such processing, even if another parent has given written consent.

Individuals can object to participation in the academy's biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted.

Academies must provide reasonable alternative means of accessing services for those individuals who will not be using an automated biometric recognition system. The Trust will comply with any guidance or advice issued by the Department for Education on the use of biometric data from time to time.

Alternative arrangements will be provided to any individual that does not consent to take part in a biometric system(s).

Alternative arrangements

All individuals have the right to not take part in a biometric system(s). Where an individual objects to taking part in the Trust's/ academy's biometric system(s), reasonable alternative arrangements will be provided that allow the individual to access the relevant service. Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service or result in any additional burden being placed on the individual (and the pupil's parents, where relevant).

Biometric data will be managed and retained in line with the Trust's Management and Retention Records Policy.

There are appropriate and robust security measures in place to protect the biometric data held by the Trust.

13. CCTV and photography

The Trust and its academies understand that recording images of identifiable individuals constitutes as processing personal information, so it must be following the Legislation and the ICO's Code of Practice on surveillance.

Where CCTV is used at an academy, the academy must notify all pupils, staff, contractors, and visitors of the purpose for collecting CCTV images via signage and its CCTV policy.

Cameras must only be placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All CCTV footage will be kept for up to six months for security purposes; the Headteacher is responsible for ensuring that the records are kept secure and for allowing access.

Each academy will always indicate its intentions for taking photographs of pupils and will obtain consent from the parent or pupil as appropriate to take the photographs and before publishing them. Where the academy wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the usage from the parent of the pupil.

Precautions, as outlined in the academy's Photography Policy, are taken when publishing photographs of pupils, in print, video or on the school website.

14. [NEW] Cloud computing

[NEW] For the purposes of this policy, 'cloud computing' refers to storing and accessing data and programs, such as documents, photos, or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the Trust and its academies accessing a shared pool of ICT services remotely via a private network or the internet.

[NEW] All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

[NEW] If the cloud service offers an authentication process, each user will have their own account. A system will be implemented to allow user accounts to be created, updated, suspended, and deleted, and for credentials to be reset if they are forgotten, lost, or stolen. Access for employees will be removed when they leave the Trust.

[NEW] All files and personal data will be encrypted before they leave a Trust device and are placed in the cloud, including when the data is 'in transit' between the device and cloud. A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. The loss of an encryption key will be reported to the DPO immediately; failure to do so could result in accidental access or destruction of personal data and, therefore, a breach of the relevant data protection legislation.

[NEW] The DPO will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services.

15. Authorised disclosures

The Trust will only disclose data about individuals if one of the lawful bases apply.

Only authorised and trained staff are allowed to make external disclosures of personal data. The Trust and its academies will regularly share personal data with third parties where it is lawful and appropriate to do so including, but not limited to, the following:

- Local Authorities.
- The Department for Education.
- The Education & Skills Funding Agency.
- The Diocese of Rochester.
- The Disclosure and Barring Service.
- The Teaching Regulation Agency.
- The Teachers' Pension Service.
- The Local Government Pension Scheme.
- Our external HR provider.
- Our external IT Provider.
- Our internal and external auditors.
- HMRC.
- The Police or other law enforcement agencies.
- Our legal advisors and other consultants.
- Insurance providers / the Risk Protection Arrangement.
- Occupational health advisors.
- Exam boards.
- The Joint Council for Qualifications.
- NHS health professionals including educational psychologists and school nurses.
- Education Welfare Officers.
- Courts, if ordered to do so.

- Prevent teams in accordance with the Prevent Duty on schools.
- Other schools, for example, if we are negotiating a managed move and we have Consent to share information in these circumstances.
- Confidential waste collection companies.
- Independent Admission Appeal Panels.
- Independent Review Panels.
- Our trip organisers such as PGL, Travel Bound and Rock UK.

Some of the organisations we share personal data with may also be data controllers in their own right in which case we will be jointly controllers of personal data and may be jointly liable in the event of any data breaches.

Data Sharing Agreements should be completed when setting up 'on-going' or 'routine' information sharing arrangements with third parties who are Data Controllers in their own right. However, they are not needed when information is shared in one-off circumstances but a record of the decision and the reasons for sharing information should be kept. All Data Sharing Agreements must be signed off by the Trust DPO who will keep a register of all Data Sharing Agreements.

The Legislation requires Data Controllers to have a written contract in place with data processors which must include specific clauses relating to the way in which the data is processed. It will be the responsibility of the academy entering into the contract to ensure that the necessary clauses have been added to the contract with the data processor. Personal data may only be transferred to a third-party data processor if they agree to put in place adequate technical, organisational and security measures themselves.

In some cases, data processors may attempt to include additional wording when negotiating contracts which attempts to allocate some of the risk relating to compliance with the Legislation, including responsibility for any Personal Data Breaches, onto the Trust. In these circumstances, the member of staff dealing with the contract should contact the Trust DPO for further advice before agreeing to include such wording in the contract.

Any personal data transferred to or from a data controller within the EEA will be undertaken by the Trust in accordance with data protection principles with the appropriate levels of security and in accordance with guidance issued by the ICO. As and when the United Kingdom leaves the EU, academies will ensure that the necessary contracts are in place with the standard contractual clauses as required by the GDPR, thereby ensuring that the transfer of personal data to and from the EEA conform with the requirements of the ICO.

[NEW] Safeguarding

[NEW] The Trust understands that the Legislation does not prevent or limit the sharing of information for the purposes of keeping children safe.

[NEW] The Trust and its academies will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is

doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate.

[NEW] The academies will aim to gain consent to share information where appropriate; however, will not endeavour to gain consent if to do so would place a child at risk. The academies will manage all instances of data sharing for the purposes of keeping a child safe in line with the relevant Child Protection and Safeguarding Policies.

16. Training

We are required to ensure all Trust personnel have undergone adequate training to enable us to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

Members of staff must attend all mandatory data privacy related training.

17. Data retention

Data will not be kept for longer than is necessary. Data that is no longer required will be deleted or destroyed securely as soon as practicable. Some educational records relating to former pupils or employees may be kept for an extended period for legal reasons or in accordance with our insurance policies, but also to enable the provision of references or academic transcripts. Data will be managed and retained in accordance with the Trust's Management and Retention of Documents Policy.

18. Complaints

Complaints about the operation of these procedures should be made to the Trust's DPO where it relates to a request made to the Trust and to the academy DPL of the relevant academy where the request for data was made to the academy. The academy DPL will liaise with the Trust DPO as appropriate. The complaint will then be dealt with pursuant to the Trust or academy complaints policy as appropriate. Where the complainant is not satisfied with the outcome of the complaint, the matter can be referred to the ICO.

19. Contacts

Anyone with concerns or questions in relation to this policy should contact the Trust DPO by:

- emailing info@aquinastrust.org and inserting data protection in the subject box; or

- writing to the Trust DPO at Aquinas Church of England Education Trust, c/o Bishop Justus CE School, Magpie Hall Lane, Bromley, Kent BR2 8HZ.

20. Monitoring and review

[UPDATED] This policy is reviewed on a **biennial** basis by the **Trust Board** and **Chief Executive**. Changes to this policy are communicated to relevant stakeholders.

The next scheduled review date for this policy is **October 2025**.