AQUINAS Church of England Education Trust

"Life - Transforming - Learning"

Policy Title:	Data Protection
Responsibility:	Chief Executive Officer
Review Body:	Board of Trustees
Date:	June 2018
Review:	June 2020

RATIONALE

The 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 come into contact with 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 General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA) collectively referred to as the legislation. This policy is in place to ensure all staff 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.

DATA PROTECTION PRINCIPLES

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.

Sensitive 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.

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 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.

TRUST PRACTICE

The Trust will operate through appropriate management and the strict application of criteria and controls in order to:

- 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 is 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.

Sensitive Personal Data

The Trust will be processing sensitive 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 sensitive personal data.

When sensitive 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, on the basis of 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 sensitive 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 sensitive personal data.

Biometric Data

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 a pupil's photo is scanned automatically to provide him or her with services. Biometric data is a type of sensitive personal data.

Where biometric data relating to pupils is processed, the relevant academy must ensure that each parent of a child is notified of the school'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. An academy must not process the biometric data if 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;
- 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.

Academies must provide reasonable alternative means of accessing services for those pupils 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.
The Trust and / or the relevant academies must obtain the explicit consent of staff, trustees or other data subjects before processing their biometric data.

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 as a result 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 the course of 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.

POLICIES RELATING TO DATA PROTECTION
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.
In particular, this policy should be read in conjunction with the Trust's:

- IT Policy detailing the data security regime;
- Management and Retention of Documents policy detailing the management and retention of documents scheme;
- Critical Incident and Business Recovery Policy.

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 with regard to 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. In the event that 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.
- In order 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 in order to avoid conflicts of interests:

- draw up internal rules to this effect in order 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 with regard to 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.

The responsibility for data protection at each academy has been delegated by Trustees to the headteacher of the academy. In order to assist headteachers with the discharge of these responsibilities, academy data protection leads (academy DPL) have been appointed for each academy as follows:

Academy	Academy Data Protection Lead	Contact Details
Bishop Justus CE School	Juliana Poloczanska	sbm@bishopjustus.bromley.sch.uk
Cudham CE Primary School	Heather Peck and Yvonne Corneille	admin@cudham.bromley.sch.uk
Keston CE Primary School	Jennifer Davall	admin@keston.bromley.sch.uk
Parish CE Primary School	Juliana Poloczanska	sbm@parish.bromley.sch.uk
St. George's CE Primary School	Anne Browne	admin@st-georgesbickley.bromley.sch.uk
St. John's CE Primary School	Pietra Salmasi and Jan 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	Lin Beattie	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.
- Alerting the CEO and Trust DPO where there has been a security breach in relation to personal data held at the academy.

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. Where a privacy notice has been provided prior to the implementation of the GDPR, the privacy notices will be refreshed where they are not GDPR compliant prior to 25 May 2018.
   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.

2. 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 must be responded to within 1 month, this period may be extended to 2 months where the request is complex, but the individual will be kept informed. The individual has a right of complaint to the ICO where the request is not complied with in this time frame.
3. 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 to 2 months where the request is complex, but the individual will be kept informed. The individual has a right of complaint to the ICO where the request for rectification is not actioned.
4. An individual may request the deletion or removal of their personal data where:
    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 personal data has to be erased to comply with a legal obligation.

    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.
5. An individual can object to processing where the condition for processing relied upon by the Trust is the performance of a task in the public interest such as the provision of education in the public interest. The Trust will only continue to process where there are compelling grounds for doing so which override the right of the individual or there are legal reasons for processing.
6. 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 make a determination. Use can also be restricted where processing is unlawful or no longer necessary but the personal data is being retained for legal reasons. Where personal data has been disclosed to a third party, they will be informed about the restriction on the processing, unless it is impossible or involves disproportionate effort to do so.
7. The Trust will also provide the individual's personal data in a portable IT format so that it can be used by the individual.

Details of the individual's rights will be included in the privacy notice provided by the Trust to pupils, parents, staff, contractors and volunteers.

Consent to Processing by an Individual

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 may consent by virtue of a positive, clear, specific affirmation to processing. Where a pupil is under the age of 13, the consent of parents will be sought prior to the processing of their data unless another lawful basis for processing the personal data applies. In the event that 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. An individual is entitled to withdraw consent at any time. A record of the consents provided will be maintained.
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.

Request for Personal data (Subject Access Request)
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 back 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. Where the request is complex or involves a large volume of information, the period can be extended to 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 in order 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.

MANAGEMENT OF PERSONAL DATA

1. The Trust and academies maintain personal data in accordance with the principles detailed in the Legislation and the practices detailed above.
2. 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.
3. Personal data is retained for as long as is necessary in order to satisfy the purpose for which it is collected or in order to comply with a legal obligation. Retention periods for personal and other data is detailed in the Trust's document management and retention policy.
4. Personal data processed by the Trust and its academies in a paper format is held securely within the relevant Trust site.
5. Personal data processed by the Trust and its academies in a digital format is held securely in accordance with the Trust's IT policy.

PRIVACY BY DESIGN AND PRIVACY 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.

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.

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 sensitive 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. Paper records
    - Personal data held in hard copy format will be kept in a locked filing cabinet, drawer, safe or similar in order 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 kept secure at all times. 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. Digital records
    - 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 closed 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 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.
    - When sending confidential information by fax, staff will always check that the recipient is correct before sending.
    - 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 supervised at all times.
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.

BREACH OF DATA SECURITY

In the event that 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 Estates and Facilities, 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:
   a) Assessing any breach of personal data security by identifying the issues and the extent of the breach as a matter of urgency.
   b) Speak to all the parties involved in the breach.
   c) Consider the physical and IT consequences of a breach of data security.
   d) 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.
   e) Secure the appropriate forensic investigation to ascertain the extent of the breach.
   f) Agree a communication strategy to deal with the PDB.
   g) Consider the harm caused by the breach of data security.
   h) Report to the police if appropriate.
   i) Keep records of the response.
   j) Notify the Information Commissioner's Office within 72 hours of the breach if appropriate.
   k) 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:

a) The nature of the personal data breach including categories and number of individuals concerns and the categories and numbers of personal data records affected.
b) Name and contact details of the DPO.
c) Description of the likely consequences of the breach; and

d) Description of the measures taken or proposed to be taken to deal with the breach and the mitigation to limit any adverse effect.

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.

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.

CCTV AND PHOTOGRAPHY

1. The Trust and its academies understand that recording images of identifiable individuals constitutes as processing personal information, so it has to be in compliance with the Legislation and the ICO's Code of Practice on surveillance.
2. 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 it CCTV policy.
3. Cameras must only be placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
4. 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.
5. Each academy will always indicate its intentions for taking photographs of pupils and will obtain consent from the parent or pupil as appropriate in order 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 particular usage from the parent of the pupil.
6. Precautions, as outlined in the academy's Photography Policy, are taken when publishing photographs of pupils, in print, video or on the school website.

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;
- 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.

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.

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

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.

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.

POLICY REVIEW

This policy is reviewed every two years by the Trust's DPO and the CEO and amendments will be recommended to Trustees.