	AAT GENERAL DATA PROTECTION REGULATION POLICY (GDPR)			
Alban Academies Trust	**Last reviewed: Jan 2019**	**Next Review: Jan 2022**	**Approved by committee**	**HR**

1. Policy statement and objectives

1.1 The objectives of this Data Protection Policy are to ensure that Alban Academies Trust (the "Trust") and its directors, governors, members and employees are informed about, and comply with, their obligations under the General Data Protection Regulation ("the GDPR") and other Data Protection legislation.

1.2 The Trust is a Multi Academy Trust with a number of academies and is the Data Controller for all the Personal Data Processed by its academies and by the central team at the Trust. For a list of the academies within the Trust, please follow this link: https://www.albanacademiestrust.org.uk/

1.3 Everyone has rights with regard to how their personal information is handled. During the course of our activities we will Process personal information about a number of different groups of people and we recognise that we need to treat it in an appropriate and lawful manner. This personal information is collected by the academies within the Trust but also by the central team who work for the Trust.

1.4 The type of information that we may be required to handle include details of job applicants, current, past and prospective employees, pupils, parents / carers and other members of pupils' families, directors, governors, members suppliers and other individuals that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the GDPR and other legislation. The GDPR imposes restrictions on how we may use that information.

1.5 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 members of staff will be taken seriously and may result in disciplinary action and serious breaches may result in dismissal. Breach of the GDPR may expose the Trust to enforcement action by the Information Commissioner's Office (ICO) or fines. Furthermore, certain breaches of the Act can give rise to personal criminal liability for the Trust's employees. At the very least, a breach of the GDPR could damage our reputation and have serious consequences for the Trust and for our stakeholders.

2. Status of the policy

2.1 This policy has been approved by the directors of the Trust. It sets out our rules on Data Protection and the legal conditions that must be satisfied in relation to the obtaining, handling, Processing, storage, transportation and destruction of personal information.

3. Data Protection Officer

3.1 The Data Protection Officer (the "DPO") is responsible for ensuring the Trust is compliant with the GDPR and with this policy. An officer at each academy holds this post. See Appendix 2 for details. Any questions or concerns about the operation of this policy should be referred in the first instance to the DPO at the relevant academy.

3.2 The DPO will play a major role in embedding essential aspects of the GDPR into the Trust's culture, from ensuring the Data Protection principles are respected to preserving Data Subject rights, recording Data Processing activities and ensuring the security of Processing.

3.3 The DPO should be involved, in a timely manner, in all issues relating to the protection of Personal Data. To do this, the GDPR 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:

3.3.1 senior management support;

3.3.2 time for DPOs to fulfil their duties;

3.3.3 adequate financial resources, infrastructure (premises, facilities and equipment) and staff where appropriate;

3.3.4 official communication of the designation of the DPO to make known existence and function within the organisation;

3.3.5 access to other services, such as HR, IT and security, who should provide support to the DPO;

3.3.6 continuous training so that DPOs can stay up to date with regard to Data Protection developments;

3.3.7 where a DPO team is deemed necessary, a clear infrastructure detailing roles and responsibilities of each team member;

3.3.8 whether the Trust should give the DPO access to external legal advice to advise the DPO on their responsibilities under this Data Protection Policy.

3.4 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.

3.5 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.

3.6 The requirement that the DPO reports directly to the board of directors ensures that the Trust's directors are made aware of the 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 of directors and to any other decision makers.

3.7 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.

3.8 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.

3.9 In the light of this and in the event that the Trust decides to appoint an internal DPO, the Trust will take the following action in order to avoid conflicts of interests:

3.9.1 identify the positions incompatible with the function of DPO;

3.9.2 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;

3.9.3 include a more general explanation of conflicts of interests;

3.9.4 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;

3.9.5 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.

3.10 If you consider that the policy has not been followed in respect of Personal Data about yourself or others you should raise the matter with the DPO.

4. Definition of terms

4.1 **Biometric Data** means Personal Data resulting from specific technical Processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images;

4.2 **Consent** of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her;

4.3 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems or other media such as CCTV;

4.4 **Data Subjects** for the purpose of this policy include all living individuals about whom we hold Personal Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Personal Data.

4.5 **Data Controllers** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

4.6 **Data Users** include employees, volunteers, trustees [and governors] whose work involves using Personal Data. Data Users have a duty to protect the information they handle by following our Data Protection and security policies at all times;

4.7 **Data Processors** means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Data Controller;

4.8 **Parent** has the meaning given in the Education Act 1996 and includes any person having parental responsibility or care of a child;

4.9 **Personal Data** means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

4.10 **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed;

4.11 **Privacy by Design** means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR;

4.12 **Processing** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

4.13 **Sensitive Personal Data** means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, Biometric Data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

5. Data Protection principles

5.1 Anyone Processing Personal Data must comply with the enforceable principles of good practice. These provide that Personal Data must be:

5.1.1 Processed lawfully, fairly and in a transparent manner in relation to individuals;

5.1.2 ollected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes; further Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

5.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed;

5.1.4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are Processed, are erased or rectified without delay;

K5.1.5 ept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are Processed; Personal Data may be stored for longer periods insofar as the Personal Data will be Processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

5.1.6 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.

6. Processed lawfully, fairly and in a transparent manner:

6.1 The GDPR is intended not to prevent the Processing of Personal Data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject. The Data Subject must be told who the Data Controller is (in this case the Trust), who the Data Controller's representative is (in this case the DPO), the purpose for which the Data is to be Processed by us, and the identities of anyone to whom the Data may be disclosed or transferred.

6.2 For Personal Data to be Processed lawfully, certain conditions have to be met. These may include:

6.2.1 where we have the Consent of the Data Subject;

6.2.2 where it is necessary for compliance with a legal obligation;

6.2.3 where Processing is necessary to protect the vital interests of the Data Subject or another person;

6.2.4 where it 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.

6.3 Personal Data may only be Processed for the specific purposes notified to the Data Subject when the Data was first collected, or for any other purposes specifically permitted by the Act. This means that Personal Data must not be collected for one purpose and then used for another. If it becomes

necessary to change the purpose for which the Data is Processed, the Data Subject must be informed of the new purpose before any Processing occurs.

6.4 Sensitive Personal Data

6.4.1 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. Therefore, Data Users must be more careful with the way in which we Process Sensitive Personal Data.

6.4.2 When Sensitive Personal Data is being Processed, as well as establishing a lawful basis (as outlined in paragraph 0 above), a separate condition for Processing it must be met. In most cases the relevant conditions are likely to be that:

6.4.2.1 the Data Subject's explicit Consent to the Processing of such Data has been obtained

6.4.2.2 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;

6.4.2.3 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;

6.4.2.4 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.

6.4.3 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.

6.5 Biometric Data

6.5.1 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.

6.5.2 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 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:

6.5.2.1 the child (whether verbally or non-verbally) objects or refuses to participate in the Processing of their Biometric Data;

6.5.2.2 no Parent has consented in writing to the Processing; or

6.5.2.3 a Parent has objected in writing to such Processing, even if another Parent has given written Consent.

6.5.3 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.

6.5.4 The Trust and / or the relevant academies must obtain the explicit Consent of staff or other Data Subjects before Processing their Biometric Data.

6.6 Criminal convictions and offences

6.6.1 There are separate safeguards in the GDPR for Personal Data relating to criminal convictions and offences.

6.6.2 It is likely that the Trust and its academies will Process Data about criminal convictions or offences. This may be as a result of pre-vetting checks we are required to undertake on staff, trustees and [governors] or due to information which we may acquire during the course of their employment or appointment.

6.6.3 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.

6.6.4 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 Data secure.

6.7 Transparency

6.7.1 One of the key requirements of the GDPR relates to transparency. This means that the Trust must keep Data Subjects informed about how their Personal Data will be Processed when it is collected.

6.7.2 One of the ways we provide this information to individuals is through a privacy notice which sets out important information what we do with their Personal Data. The Trust has developed privacy notices for the following categories of people:

6.7.2.1 Pupils

6.7.2.2 Parents

6.7.2.3 Staff

6.7.2.4 Trustees / governors.

6.7.3 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.

6.7.4 We will ensure that privacy notices are concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge.

6.8 Consent

6.8.1 The Trust must only Process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent. Consent is not the only lawful basis and there are likely to be many circumstances when we Process Personal Data and our justification for doing so is based on a lawful basis other than Consent.

6.8.2 A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

6.8.3 In the event that we are relying on Consent as a basis for Processing Personal Data about pupils, if a pupil is aged under 13, we will need to obtain Consent from the Parent(s). 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 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.

6.8.4 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if we intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

6.8.5 Unless we can rely on another legal basis of Processing, explicit Consent is usually required for Processing Sensitive Personal Data. Often we will be relying on another legal basis (and not require explicit Consent) to Process most types of Sensitive Data.

6.8.6 Evidence and records of Consent must be maintained so that the Trust can demonstrate compliance with Consent requirements.

7. Specified, explicit and legitimate purposes

7.1 Personal Data should only be collected to the extent that it is required for the specific purpose notified to the Data Subject, for example, in the Privacy Notice or at the point of collecting the Personal Data. Any Data which is not necessary for that purpose should not be collected in the first place.

7.2 The Trust will be clear with Data Subjects about why their Personal Data is being collected and how it will be Processed. We cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have consented where necessary.

8. Adequate, relevant and limited to what is necessary

8.1 The Trust will ensure that the Personal Data collected is adequate to enable us to perform our functions and that the information is relevant and limited to what is necessary.

8.2 In order to ensure compliance with this principle, the Trust will check records at appropriate intervals for missing, irrelevant or seemingly excessive information and may contact Data Subjects to verify certain items of Data.

8.3 Trust employees must also give due consideration to any forms stakeholders are asked to complete and consider whether all the information is required. We may only collect Personal Data that is needed to operate as a business function and we should not collect excessive Data. We should ensure that any Personal Data collected is adequate and relevant for the intended purposes.

8.4 The Trust will implement measures to ensure that Personal Data is Processed on a 'Need to Know' basis. This means that the only members of staff, governors or trustees who need to know Personal Data about a Data Subject will be given access to it and no more information than is necessary for the relevant purpose will be shared. In practice, this means that the Trust may adopt a layered approach in some circumstances, for example, members of staff, trustees or governors may be given access to basic information about a pupil or employee if they need to know it for a particular purpose but other information about a Data Subject may be restricted to certain members of staff who need to know it, for example, where the information is Sensitive Personal Data, relates to criminal convictions or offences or is confidential in nature (for example, child protection or safeguarding records).

8.5 When Personal Data is no longer needed for specified purposes, it must be deleted or anonymised in accordance with the Trust's Data Retention guidelines.

9. Accurate and, where necessary, kept up to date

9.1 Personal Data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date Data should be destroyed.

9.2 If a Data Subject informs the Trust of a change of circumstances their records will be updated as soon as is practicable.

9.3 Where a Data Subject challenges the accuracy of their Data, the Trust will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Chair of Governors on the Local Governing Body for their judgement. If the problem cannot be resolved at this stage, the Data Subject should refer their complaint to the Information Commissioner's Office. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

9.4 Notwithstanding paragraph 0, a Data Subject continues to have rights under the GDPR and may refer a complaint to the Information Commissioner's Office regardless of whether the procedure set out in paragraph 0 has been followed.

10. Data to be kept for no longer than is necessary for the purposes for which the Personal Data are Processed

10.1 Personal Data should not be kept longer than is necessary for the purpose for which it is held. This means that Data should be destroyed or erased from our systems when it is no longer required.

10.2 It is the duty of the DPO, after taking appropriate guidance for legal considerations, to ensure that obsolete Data is properly erased. The Trust has a retention schedule for all Data.

11. Data to be Processed in a manner that ensures appropriate security of the Personal Data

11.1 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.

11.2 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.

11.3 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.

11.4 The GDPR 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. Data Users must follow all these procedures and technologies and must comply with all applicable aspects of our academies IT use and data security policies and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

11.5 Maintaining Data Security means guaranteeing the confidentiality, integrity and availability of the Personal Data, defined as follows:

11.5.1 **Confidentiality** means that only people who are authorised to use the Data can access it.

11.5.2 **Integrity** means that Personal Data should be accurate and suitable for the purpose for which it is Processed.

11.5.3 **Availability** means that authorised users should be able to access the Data if they need it for authorised purposes.

11.6 It is the responsibility of all members of staff, trustees and governors 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 DPO.

11.7 Please see each academy website for their Data Security Policy for details for the arrangements in place to keep Personal Data secure

11.8 Trustees and governors

11.8.1 Trustees and Governors are likely to Process Personal Data when they are performing their duties, for example, if they are dealing with employee issues, pupil exclusions or Parent complaints. Trustees and Governors should be trained on the Trust's Data Protection Processes as part of their induction and should be informed about their responsibilities to keep Personal Data secure. This includes:

11.8.1.1 Ensure that Personal Data which comes into their possession as a result of their Trustee or Governor duties is kept secure from third parties, including family members and friends;

11.8.1.2 Ensure they are provided with a copy of the academy's Data Security Policy.

11.8.1.3 Using a Trust email account for any Trust-related communications;

11.8.1.4 Ensuring that any Trust-related communications or information stored or saved on an electronic device or computer is password protected;

11.8.1.4 Taking appropriate measures to keep Personal Data secure, which includes ensuring that hard copy documents are securely locked away so that they cannot be accessed by third parties.

11.8.2 Trustees and Governors will be asked to read and sign an Acceptable Use Agreement.

12. Processing in line with Data Subjects' rights

12.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

12.1.1 withdraw Consent to Processing at any time;

12.1.2 receive certain information about the Data Controller's Processing activities;

12.1.3 request access to their Personal Data that we hold;

12.1.4 prevent our use of their Personal Data for direct marketing purposes;

12.1.5 ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate Data or to complete incomplete Data;

12.1.6 strict Processing in specific circumstances;

12.1.7 challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

12.1.8 request a copy of an agreement under which Personal Data is transferred outside of the EEA;

12.1.9 object to decisions based solely on Automated Processing, including profiling (Automated Decision Making);

12.1.10 prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

12.1.11 be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

12.1.12 make a complaint to the supervisory authority (the ICO); and

12.1.13 in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

12.2 We are required to verify the identity of an individual requesting Data under any of the rights listed above. Members of staff should not allow third parties to persuade them into disclosing Personal Data without proper authorisation.

13. Dealing with Subject Access Requests

13.1 The GDPR extends to all Data Subjects a right of access to their own Personal Data. A formal request from a Data Subject for information that we hold about them must be made in writing. The Trust or its academies can invite a Data Subject to complete a form but we may not insist that they do so.

13.2 It is important that all members of staff are able to recognise that a written request made by a person for their own information is likely to be a valid Subject Access Request, even if the Data Subject does not specifically use this phrase in their request or refer to the GDPR. In some cases, a Data Subject may mistakenly refer to the "Freedom of Information Act" but this should not prevent an Academy or the Trust from responding to the request as being made under the GDPR, if appropriate. Some requests may contain a combination of a Subject Access Request for Personal Data under the GDPR and a request for information under the Freedom of Information Act 2000 ("FOIA"). Requests for information under the FOIA must be dealt with promptly and in any event within 20 school days.

13.3 Any member of staff who receives a written request of this nature must immediately forward it to the Academy DPO as the statutory time limit for responding is **one calendar month**.

13.4 As the time for responding to a request does not stop during the periods when an academy is closed for the holidays, we will attempt to mitigate any impact this may have on the rights of Data Subjects to request access to their Data by periodically checking the DPO email inbox during the summer holidays.

13.5 A fee may no longer be charged to the individual for provision of this information (previously a fee of £10 could be charged under the DPA 1998).

13.6 The Academy or central team at the Trust may ask the Data Subject for reasonable identification so that they can satisfy themselves about the person's identity before disclosing the information.

13.7 In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place.

13.8 Requests from pupils who are considered mature enough to understand their rights under the GDPR will be Processed as a Subject Access Request as outlined below and the Data will be given directly to the pupil (subject to any exemptions that apply under the GDPR or other legislation). As the age when a young person is deemed to be able to give Consent for online services is 13, we will use this age as a guide for when pupils may be considered mature enough to exercise their own subject access rights. In every case it will be for the Trust, as Data Controller, to assess whether the child is capable of understanding their rights under the GDPR and the implications of their actions, and so decide whether the Parent needs to make the request on the child's behalf. A Parent would normally be expected to make a request on a child's behalf if the child is younger than 13 years of age.

13.9 Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.

13.10 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). If the Parent makes a request for their child's Personal Data and the child is aged 13 or older and / or the Trust considers the child to be mature enough to understand their rights under the GDPR, the Trust shall ask the pupil for their Consent to disclosure of the Personal Data 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.

13.11 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).

13.12 Following receipt of a Subject Access Request, and provided that there is sufficient information to Process the request, an entry should be made in the Trust's Subject Access log book, showing the date of receipt, the Data Subject's name, the name and address of requester (if different), the type of Data required (e.g. Student Record, Personnel Record), and the planned date for supplying the information (not more than one calendar month from the request date). Should more information be required to establish either the identity of the Data Subject (or agent) or the type of Data requested, the date of entry in the log will be date on which sufficient information has been provided.

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

13.13.1 charge a reasonable fee taking into account the administrative costs of providing the information; or

13.13.2 refuse to respond.

13.14 Where we refuse to respond to a request, the response must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month. Members of staff should refer to any guidance issued by the ICO on Subject Access Requests [and consult the DPO] before refusing a request.

13.15 Certain information may be exempt from disclosure so members of staff will need to consider what exemptions (if any) apply and decide whether you can rely on them. For example, information about third parties may be exempt from disclosure. In practice, this means that you may be entitled to withhold some documents entirely or you may need to redact parts of them. Care should be taken to ensure that documents are redacted properly. Please seek further advice or support from the DPO if you are unsure which exemptions apply.

13.16 In the context of an Academy a Subject Access Request is normally part of a broader complaint or concern from a Parent or may be connected to a disciplinary or grievance for an employee. Members of staff should therefore ensure that the broader context is taken into account when responding to a request and seek advice if required on managing the broader issue and the response to the request.

14. Providing information over the telephone

14.1 Any member of staff dealing with telephone enquiries should be careful about disclosing any Personal Data held by the Trust whilst also applying common sense to the particular circumstances. In particular they should:

14.1.1 Check the caller's identity to make sure that information is only given to a person who is entitled to it.

14.1.2 Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

14.1.3 Refer to their line manager or the DPO for assistance in difficult situations. No-one should feel pressurised into disclosing personal information.

15. Authorised disclosures

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

15.2 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:

15.2.1 Local Authorities

15.2.2 the Department for Education

15.2.3 the Education & Skills Funding Agency

15.2.4 the Disclosure and Barring Service

15.2.5 the Teaching Regulation Agency

15.2.6 the Teachers' Pension Service

15.2.7 the Local Government Pension Scheme which is administered by Hertfordshire County Council

15.2.8 our external HR provider

15.2.9 our external payroll provider

15.2.10 Our external IT Provider

15.2.11 HMRC

15.2.12 the Police or other law enforcement agencies

15.2.13 our legal advisors and other consultants

15.2.14 insurance providers / the Risk Protection Arrangement

15.2.15 occupational health advisors

15.2.16 exam boards including OCR, AQA, Edexcel, WJEC and other accredited awarding bodies;

15.2.17 the Joint Council for Qualifications;

15.2.18 NHS health professionals including educational psychologists, CAMHS and school nurses;

15.2.19 Education Welfare Officers;

15.2.20 Courts, if ordered to do so;

15.2.21 Prevent teams in accordance with the Prevent Duty on schools;

15.2.22 other schools, for example, if we are negotiating a managed move and we have Consent to share information in these circumstances;

15.2.23 confidential waste collection companies;

15.2.24 systems and companies that we use to communicate with parents and collect payments e.g. Parentmail, ParentPay, Wisepay, Bromcom;

15.2.25 Universities and Colleges Admissions Service (UCAS);

15.2.26 YC Hertfordshire in relation to careers advice, work experience or support services;

15.2.27 Agencies that provide family support and attendance improvement services such as Herts for Learning, St Albans Plus and others

15.3 Some of the organisations we share Personal Data with may also be Data Controllers in their own right in which case we will be joint controllers of Personal Data and may be jointly liable in the event of any Data Breaches.

15.4 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.

15.54 All Data Sharing Agreements must be signed off by the Data Protection Officer who will keep a register of all Data Sharing Agreements.

15.6 The GDPR 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 ("GDPR clauses"). A summary of the GDPR clauses is set out in Appendix 1. It will be the responsibility of the Academy entering into the contract to ensure that the GDPR 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.

15.7 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 GDPR, including responsibility for any Personal Data Breaches, onto the Trust. In these circumstances, the member of staff dealing with the contract should contact the DPO for further advice before agreeing to include such wording in the contract.

16. Reporting a Personal Data Breach

16.1 The GDPR requires Data Controllers to notify any Personal Data Breach to the ICO and, in certain instances, the Data Subject.

16.2 A notifiable Personal Data Breach must be reported to the ICO without undue delay and where feasible within 72 hours, unless the Data Breach is unlikely to result in a risk to the individuals.

16.3 If the breach is likely to result in high risk to affected Data Subjects, the GDPR, requires organisations to inform them without undue delay.

16.4 It is the responsibility of the DPO, or the nominated deputy, to decide whether to report a Personal Data Breach to the ICO.

16.5 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

16.6 The Trust recognises that as our academies are closed or have limited staff available during school holidays, there will be times when our ability to respond to a Personal Data Breach promptly and within the relevant timescales will be affected. We will consider any proportionate measures that we can implement to mitigate the impact this may have on Data Subjects when we develop our policies for response at Academy level.

16.7 If a member of staff, trustee or governor knows or suspects that a Personal Data Breach has occurred, the Academy response plan must be followed. In particular, the DPO must be notified immediately. You should preserve all evidence relating to the potential Personal Data Breach.

17. Accountability

17.1 The Trust must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with Data Protection principles. The Trust is responsible for, and must be able to demonstrate, compliance with the Data Protection principles.

17.2 The Trust must have adequate resources and controls in place to ensure and to document GDPR compliance including:

17.2.1 appointing a suitably qualified DPO (where necessary) and an executive team accountable for Data Privacy;

17.2.2 implementing Privacy by Design when Processing Personal Data and completing Data Protection Impact Assessments (DPIAs) where Processing presents a high risk to rights and freedoms of Data Subjects;

17.2.3 integrating Data Protection into internal documents including this Data Protection Policy, related policies and Privacy Notices;

17.2.4 regularly training Trust employees, trustees and [governors] on the GDPR, this Data Protection Policy, related policies and Data Protection matters including, for example, Data Subject's rights, Consent, legal bases, DPIA and Personal Data Breaches. The Trust must maintain a record of training attendance by Trust personnel; and

17.2.5 regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

18. Record keeping

18.1 The GDPR requires us to keep full and accurate records of all our Data Processing activities.

18.2 We must keep and maintain accurate records reflecting our Processing including records of Data Subjects' consents and procedures for obtaining consents.

18.3 These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

19. Training and audit

19.1 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.

19.2 Members of staff must attend all mandatory Data Privacy related training.

20. Privacy By Design and Data Protection Impact Assessment (DPIA)

20.1 We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with Data Privacy principles.

20.2 This means that we must assess what Privacy by Design measures can be implemented on all programs/systems/Processes that Process Personal Data by taking into account the following:

20.2.1 the state of the art;

20.2.2 the cost of implementation;

20.2.3 the nature, scope, context and purposes of Processing; and

20.2.4 The risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

20.3 We are also required to conduct DPIAs in respect to high risk Processing.

20.4 The Trust and its academies should conduct a DPIA and discuss the findings with the DPO when implementing major system or business change programs involving the Processing of Personal Data including:

20.4.1 use of new technologies (programs, systems or Processes), or changing technologies (programs, systems or Processes);

20.4.2 Automated Processing including profiling and Automated Decision-Making (ADM);

20.4.3 large scale Processing of Sensitive Data; and

20.4.4 large scale, systematic monitoring of a publicly accessible area.

20.5 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.

20.6 A DPIA must include:

20.6.1 a description of the Processing, its purposes and the Trust's legitimate interests if appropriate;

20.6.2 an assessment of the necessity and proportionality of the Processing in relation to its purpose;

20.6.3 an assessment of the risk to individuals; and

20.6.4 the risk mitigation measures in place and demonstration of compliance.

21. CCTV

21.1 The Trust and its academies use CCTV in locations around their sites. This is to:

21.1.1 protect the academy buildings and their assets;

21.1.2 increase personal safety and reduce the fear of crime;

21.1.3 support the Police in a bid to deter and detect crime;

21.1.4 assist in identifying, apprehending and prosecuting offenders;

21.1.5 provide evidence for the Trust to use in its internal investigations and / or disciplinary Processes in the event of behaviour by staff, pupils or other visitors on the site which breaches or is alleged to breach the Trust's policies;

21.1.6 protect members of the school community, public and private property; and

21.1.7 assist in managing the academy.

21.2 Please refer to the individual Academy's CCTV policy/code of practice for more information.

22. Policy Review

22.1. It is the responsibility of the directors to facilitate the review of this policy on a regular basis. Recommendations for any amendments should be reported to the DPO.

22.2 We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

22.3 This policy should be reviewed by the Trust periodically and at least every 2 years. It is important to ensure that the DPO is aware of his or her obligations under this policy and that they receive the training and other support they need in order to fulfil this role.

23. Enquiries

23.1 Further information about the Trust's Data Protection Policy is available from the DPO.

23.2 General information about the Act can be obtained from the Information Commissioner's Office: www.ico.gov.uk

Document Control

Date modified	Description of modification	Modified by

Appendix 1 – GDPR Clauses

The GDPR requires the following matters to be addressed in contracts with Data Processors. The wording below is a summary of the requirements in the GDPR and is not intended to be used as the drafting to include in contracts with Data Processors.

1. The Processor may only Process Personal Data on the documented instructions of the controller, including as regards international transfers. (Art. 28(3)(a))

2. Personnel used by the Processor must be subject to a duty of confidence. (Art. 28(3)(b))

3. The Processor must keep Personal Data secure. (Art. 28(3)(c) Art. 32)

4. The Processor may only use a sub-Processor with the Consent of the Data Controller. That Consent may be specific to a particular sub-Processor or general. Where the Consent is general, the Processor must inform the controller of changes and give them a chance to object. (Art. 28(2) Art. 28(3)(d))

5. The Processor must ensure it flows down the GDPR obligations to any sub-Processor. The Processor remains responsible for any Processing by the sub-Processor. (Art. 28(4))

6. The Processor must assist the controller to comply with requests from individuals exercising their rights to access, rectify, erase or object to the Processing of their Personal Data. (Art. 28(3)(e))

7. The Processor must assist the Data Controller with their security and Data Breach obligations, including notifying the Data Controller of any Personal Data Breach. (Art. 28(3)(f)) (Art. 33(2))

8. The Processor must assist the Data Controller should the Data Controller need to carry out a privacy impact assessment. (Art. 28(3)(f))

9. The Processor must return or delete Personal Data at the end of the agreement, save to the extent the Processor must keep a copy of the Personal Data under Union or Member State law. (Art. 28(3)(g))

10. The Processor must demonstrate its compliance with these obligations and submit to audits by the Data Controller (or by a third party mandated by the controller). (Art. 28(3)(h))

11. The Processor must inform the Data Controller if, in its opinion, the Data Controller's instructions would breach Union or Member State law. (Art. 28(3))

Appendix 2 – AAT member schools DPO contact details and policies

Ridgeway Academy
Patricia Diop, School Business Manager
patricia.diop@sandringham.herts.sch.uk
Policies: https://www.ridgeway.herts.sch.uk/our-school/information-and-policies/

Sandringham School
Fergal Moane, Deputy Headteacher
dpo@sandringham.herts.sch.uk
Policies: https://www.sandringham.herts.sch.uk/about-us/information-and-policies/

Verulam School
Mr Mark Kennedy
dpo@verulam.herts.sch.uk
Policies: https://verulamschool.co.uk/policies-statutory-information/