Data Protection (GDPR) Policy

December 2021

Date of Next Review – 30/11/22

Contents:

Statement of intent

1. Legal framework
2. About this policy
3. Definition of data protection terms
4. Data Protection Officer (DPO)
5. Data Protection Principles
6. Fair and Lawful processing
7. Processing for limited purposes
8. Notifying Data Subjects
9. Adequate, relevant and non-excessive processing
10. Accurate data
11. Timely Processing
12. Processing in line with data subject's rights
13. Data Security
14. Data Protection Impact Assessments
15. Disclosure and sharing of personal information
16. Data Processors
17. Images and Videos
18. CCTV
19. Biometric Data
20. Data Breach
21. DBS Data
22. Policy review

Statement of intent

The Apollo Partnership Trust is required to keep and process certain information about its workforce, pupils/students, parents and others in accordance with its legal obligations under the Data Protection Legislation consisting of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 and relevant regulations.

Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities as a Trust we will collect, store and **process personal data** about our pupils/students, **workforce**, parents and others. This makes us a **data controller** in relation to that **personal data**.

We are committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.

All members of our **workforce** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

The Trust may, from time to time, be required to share personal information about its workforce, pupils/students, parents and others with other organisations, mainly the Local Authority, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Trust complies with the following core principles of the Data Protection Legislation.

Organisational methods for keeping data secure are imperative, and The Apollo Partnership Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy does not form part of any employee's contract of employment and may be amended at any time.

This policy complies with the requirements set out in the Data Protection Legislation

1. Legal framework

1.1. This policy has due regard to legislation, including, but not limited to the following:

1.1.1. The General Data Protection Regulation

1.1.2. The Data Protection Act 2018

1.1.3. The Freedom of Information Act 2000

1.1.4. The Education (Independent School Standards) Regulations 2014

1.1.5. The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

1.2. This policy also has regard to the following guidance:

- The Department for Education's Data protection: toolkit for schools

1.2.1. The Information Commissioner's Office Guide to the General Data Protection Regulation (GDPR)

1.3. This policy will be implemented in conjunction with the following other Trust policies:

1.3.1. Photography and Videos Policy
1.3.2. E-safety Policy
1.3.3. Surveillance & CCTV Policy
1.3.4. IT Acceptable Use Policy

2. About this policy

2.1 The types of **personal data** that we may be required to handle include information about pupils/students, parents, our **workforce**, and others that we deal with. The **personal data** which we hold is subject to certain legal safeguards specified in the General Data Protection Regulation ('**GDPR**'), the [Data Protection Act 2018], and other regulations (together '**Data Protection Legislation**').

2.2 This policy and any other documents referred to in it set out the basis on which we will **process** any **personal data** we collect from **data subjects**, or that is provided to us by **data subjects** or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.

3. Definition of data protection terms

3.1 All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in the Annex to this policy.

4. Data Protection Officer

4.1 As a Trust we are required to appoint a Data Protection Officer ("DPO"). Our DPO can be contacted at dpo@apollopartnershiptrust.uk

4.2 The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

4.3 The DPO is also the central point of contact for all **data subjects** and others in relation to matters of data protection.

4.4 The DPO will report to the highest level of management at the Trust, which is the Chief Executive Officer.

5. Data Protection Principles

5.1 Anyone **processing personal data** must comply with the data protection principles. These provide that **personal data** must be:

5.1.1 **Processed** fairly and lawfully and transparently in relation to the **data subject**;

5.1.2 **Processed** for specified, lawful purposes and in a way which is not incompatible with those purposes;

5.1.3 Adequate, relevant and not excessive for the purpose;

5.1.4 Accurate and up to date;

5.1.5 Not kept for any longer than is necessary for the purpose; and

5.1.6 **Processed** securely using appropriate technical and organisational measures.

5.2 **Personal Data** must also:

5.2.1 be **processed** in line with **data subjects'** rights;

5.2.2 not be transferred to people or organisations situated in other countries without adequate protection.

5.3 We will comply with these principles in relation to any **processing** of **personal data** by the Trust.

6. Fair and Lawful processing

6.1. Data Protection Legislation is not intended 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**.

6.2. For **personal data** to be **processed** fairly, **data subjects** must be made aware:

6.2.1. that the **personal data** is being **processed**;

6.2.2. why the **personal data** is being **processed**;

6.2.3. what the lawful basis is for that **processing** (see below);

6.2.4. whether the **personal data** will be shared, and if so with whom;

6.2.5. the period for which the **personal data** will be held;

6.2.6. the existence of the **data subject's** rights in relation to the **processing** of that **personal data**; and

6.2.7. the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

6.3. We will only obtain such **personal data** as is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any **processing**.

6.4. For **personal data** to be **processed** lawfully, it must be **processed** on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally **process personal data** under the following legal grounds:

6.4.1. where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract;

6.4.2. where the **processing** is necessary to comply with a legal obligation that we are subject to, (e.g the Education Act 2011);

6.4.3. where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest; and

6.4.4. where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **personal data.**

6.5. When **special category personal data** is being processed then an additional legal ground must apply to that processing. We will normally only **process special category personal data** under following legal grounds:

6.5.1. where the **processing** is necessary for employment law purposes, for example in relation to sickness absence;

6.5.2. where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;

6.5.3. where the **processing** is necessary for health or social care purposes, for example in relation to pupils/students with medical conditions or disabilities; and

6.5.4. where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **special category personal data**.

6.6. We will inform **data subjects** of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil/student joins us.

6.7. If any **data user** is in doubt as to whether they can use any **personal data** for any purpose then they must contact the DPO before doing so.

Vital Interests

6.8. There may be circumstances where it is considered necessary to **process personal data** or **special category personal data** in order to protect the vital interests of a **data subject**. This might include medical emergencies where the **data subject** is not in a position to give consent to the **processing**. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

6.9. Where none of the other bases for **processing** set out above apply then the school must seek the consent of the **data subject** before **processing** any **personal data** for any purpose.

6.10. There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.

6.11. When pupils/students and or our Workforce join the Trust a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

6.12 In relation to all pupils/students of primary school age or in Year 7, 8 or 9, we will seek consent from an individual with parental responsibility for that pupil/student.

6.13 We will generally seek consent directly from a pupil/student who is on roll and in Year 10, 11, 12 and 13, however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from and individual with parental responsibility.

6.14 If consent is required for any other **processing** of **personal data** of any **data subject** then the form of this consent must:

6.14.1 Inform the **data subject** of exactly what we intend to do with their **personal data**;

6.14.2 Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and

6.14.3 Inform the **data subject** of how they can withdraw their consent.

6.15 Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a **data subject** giving their consent.

6.16 The DPO must always be consulted in relation to any consent form before consent is obtained.

6.17 A record must always be kept of any consent, including how it was obtained and when.

7. Processing for limited purposes

7.1 In the course of our activities as a Trust, we may collect and **process** the **personal data** set out in our Schedule of Processing Activities. This may include **personal data** we receive directly from a **data subject** (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and **personal data** we receive from other sources (including, for example, local authorities, other schools, parents, other pupils/students or members of our **workforce**).

7.2 We will only **process personal data** for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

8. Notifying Data Subjects

8.1 If we collect **personal data** directly from **data subjects**, we will inform them about:

8.1.1 our identity and contact details as **Data Controller** and those of the DPO;

8.1.2 the purpose or purposes and legal basis for which we intend to **process** that **personal data**;

8.1.3 the types of third parties, if any, with which we will share or to which we will disclose that **personal data**;

8.1.4 whether the **personal data** will be transferred outside the European Economic Area (‘**EEA**’) and if so the safeguards in place;

12.1.1 8.1.5 the period for which their **personal data** will be stored, by reference to our Retention and Destruction Schedule;

8.1.6 the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making; and

8.1.7 the rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

8.2 Unless we have already informed **data subjects** that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive **personal data** about a **data subject** from other sources, we will provide the **data subject** with the above information as soon as possible thereafter, informing them of where the **personal data** was obtained from.

9. Adequate, relevant and non-excessive processing

9.1 We will only collect **personal data** to the extent that it is required for the specific purpose notified to the **data subject**, unless otherwise permitted by Data Protection Legislation.

10. Accurate data

10.1 We will ensure that **personal data** we hold is accurate and kept up to date.

10.2 We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

10.3 **Data subjects** have a right to have any inaccurate **personal data** rectified. See further below in relation to the exercise of this right.

11. Timely Processing

11.1. We will not keep **personal data** longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all **personal data** which is no longer required.

12. Processing in line with data subject's rights

8.3 We will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:

8.3.1 request access to any **personal data** we hold about them;

12.1.2 object to the **processing** of their **personal data**, including the right to object to direct marketing;

12.1.3 have inaccurate or incomplete **personal data** about them rectified;

12.1.4 restrict **processing** of their **personal data**;

12.1.5 have **personal data** we hold about them erased

12.1.6 have their **personal data** transferred; and

12.1.7 object to the making of decisions about them by automated means.

The Right of Access to Personal Data

12.2 **Data subjects** may request access to all **personal data** we hold about them. Such requests will be considered in line with the schools Subject Access Request Procedure.

The Right to Object

12.3 In certain circumstances **data subjects** may object to us **processing** their **personal data**. This right may be exercised in relation to **processing** that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

12.4 An objection to **processing** does not have to be complied with where the school can demonstrate compelling legitimate grounds which override the rights of the **data subject**.

12.5 Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

12.6 In respect of direct marketing any objection to **processing** must be complied with.

12.7 The Trust is not however obliged to comply with a request where the **personal data** is required in relation to any claim or legal proceedings.

Automated decision making and profiling

12.8. Individuals have the right not to be subject to a decision when:

12.8.1. It is based on automated processing, e.g. profiling.

12.8.2. It produces a legal effect or a similarly significant effect on the individual.

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

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

12.10.1. Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predictedimpact.

12.10.2. Using appropriate mathematical or statistical procedures.

12.10.3. Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.

12.10.4. Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

12.11. Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

12.11.1. The Trust has the explicit consent of the individual.

12.11.2. The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

The Right to Rectification

12.12 If a **data subject** informs the Trust that **personal data** held about them by the Trust is inaccurate or incomplete then we will consider that request and provide a response within one month.

12.13 If we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary then we will inform the **data subject** within one month of their request that this is the case.

12.14 We may determine that any changes proposed by the **data subject** should not be made. If this is the case then we will explain to the **data subject** why this is the case. In those circumstances we will inform the **data subject** of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

12.15 **Data subjects** have a right to "block" or suppress the **processing** of **personal data**. This means that the Trust can continue to hold the **personal data** but not do anything else with it.

12.16 The Trust must restrict the **processing** of **personal data**:

12.16.1 Where it is in the process of considering a request for **personal data** to be rectified (see above);

12.16.2 Where the Trust is in the process of considering an objection to processing by a **data subject**;

12.16.3 Where the **processing** is unlawful but the **data subject** has asked the Trust not to delete the **personal data**; and

12.16.4 Where the Trust no longer needs the **personal data** but the **data subject** has asked the Trust not to delete the **personal data** because they need it in relation to a legal claim, including any potential claim against the Trust.

12.17 If the Trust has shared the relevant **personal data** with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

12.18 The DPO must be consulted in relation to requests under this right.

The Right to Be Forgotten

12.19 **Data subjects** have a right to have **personal data** about them held by the Trust erased only in the following circumstances:

12.19.1 Where the **personal data** is no longer necessary for the purpose for which it was originally collected;

12.19.2 When a **data subject** withdraws consent – which will apply only where the Trust is relying on the individuals consent to the **processing** in the first place;

12.19.3 When a **data subject** objects to the **processing** and there is no overriding legitimate interest to continue that **processing** – see above in relation to the right to object;

12.19.4 Where the **processing** of the **personal data** is otherwise unlawful;

12.19.5 When it is necessary to erase the **personal data** to comply with a legal obligation; and

12.20 The Trust is not required to comply with a request by a **data subject** to erase their **personal data** if the **processing** is taking place:

12.20.1 To exercise the right of freedom of expression or information;

12.20.2 To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;

12.20.3 For public health purposes in the public interest;

12.20.4 For archiving purposes in the public interest, research or statistical purposes; or

12.20.5 In relation to a legal claim.

12.21 If the Trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

12.22 The DPO must be consulted in relation to requests under this right.

Right to Data Portability

12.23 In limited circumstances a **data subject** has a right to receive their **personal data** in a machine-readable format, and to have this transferred to other organisation.

12.24 If such a request is made then the DPO must be consulted.

13.Data Security

13.1 We will take appropriate security measures against unlawful or unauthorised processing of **personal data**, and against the accidental loss of, or damage to, **personal data**.

13.2 Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

13.3 Confidential paper records will not be left unattended or in clear view anywhere with general access.

13.4 Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

13.5 Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

13.6 Memory sticks will not be used in Apollo Partnership Trust Schools.

13.7 All electronic devices are password-protected to protect the information on the device in case of theft.

13.8 Where possible, the Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.

13.9 Staff will not use their personal laptops or computers for school purposes.

13.10 All necessary Trustees, LGB members, members of staff and trainee teachers are provided with their own secure login and password, and every computer regularly prompts users to change their password, which is not to be shared and kept secure.

13.11 All necessary Trustees, LGB members, members of staff and trainee teachers are provided with their own secure email account to use for school related activity and communications.

13.12 Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

13.13 Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

13.14 When sending confidential information by fax, staff will always check that the recipient is correct before sending.

13.15 Where **personal data** 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, e.g. keeping devices under lock and key. The person taking the information from the Trust premises accepts full responsibility for the security of the data.

13.16 Before sharing **personal data**, all staff members will ensure:

13.16.1 They are allowed to share it.

13.16.2 That adequate security is in place to protect it.

13.16.3 Who will receive the data has been outlined in a privacy notice.

13.17 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Trust containing sensitive information are supervised at all times.

13.18 The physical security of the Trust'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.

13.19 The Apollo Partnership Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

13.20 The following employees are responsible for continuity and recovery measures are in place to ensure the security of protected data: CEO / CFOD / MLT / Head of Schools & Headteacher / ABM / Network Manager.

14.Data Protection Impact Assessments

14.1 The Trust takes data protection very seriously and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

14.2 In certain circumstances the law requires us to carry out detailed assessments of proposed **processing**. This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or the way that we intend to do so.

14.3 The Trust will complete a Data protection impact assessment (DPIA) of any such proposed **processing** and has a template document which ensures that all relevant matters are considered when identifying the most effective method of complying with

the Trust's data protection obligations and meeting individuals' expectations of privacy.

14.4 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 Trust's reputation which might otherwise occur.

14.5 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.

14.6 A DPIA will be used for more than one project, where necessary.

14.7 High risk processing includes, but is not limited to, thefollowing:

14.7.1 Systematic and extensive processing activities, such as profiling

14.7.2 Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

14.7.3 The use of CCTV.

14.8. The Trust will ensure that all DPIAs include the following information:

14.8.1. A description of the processing operations and the purposes

14.8.2. An assessment of the necessity and proportionality of the processing in relation to the purpose

14.8.3. An outline of the risks to individuals

14.8.4. The measures implemented in order to address risk

14.9. Where a DPIA indicates high risk data processing, the Trust will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

14.10 The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

15.Disclosure and sharing of personal information

15.1 We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, Education "DfE" and Skills Funding Agency "ESFA", Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

15.2 The Trust will inform **data subjects** of any sharing of their **personal data** unless we are not legally required to do so, for example where **personal data** is shared with the police in the investigation of a criminal offence.

15.3 In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.

15.4 Further detail is provided in our Schedule of Processing Activities.

15.5. The Apollo Partnership Trust publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

15.5.1. Policies and procedures

15.5.2. Minutes of meetings

15.5.3. Annual reports

15.5.4. Financial information

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

15.7. The Apollo Partnership Trust will not publish any personal information, including photos, on its website without the permission of the affected individual.

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

16.Data Processors

16.1 We contract with various organisations who provide services to the Trust, including:

- Local authorities, – to meet our legal obligations to share certain information such as concerns about pupils'/students' safety and exclusions or to assist them in the exercise of their responsibilities in relation to education and training, youth support, SEND and safeguarding purposes
- The Department for Education and the Education and Skills Funding Agency, in compliance with legal obligations of the school to provide information about students and parents as part of statutory data collections
- Contractors, such as payment processing providers to enable payments to be made by you to the Trust/Academy
- Educators and examining bodies
- Financial organisations
- Our auditors
- Survey and research organisations
- The Health authorities and consultants
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Contractors – to enable them to provide the service we have contracted them for, such as payroll, Strategic HR services, DBS clearance checks, Occupational Health questionnaires and referrals
- Pension providers and government agencies such as HMRC and DWP regarding tax payments and benefits

- Survey and research organisations, office for National Statistics
- Trade unions and associations
- Employment and recruitment agencies

16.2 In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

16.3 **Personal data** will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Trust. The Trust will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

16.4 Contracts with **data processors** will comply with Data Protection Legislation and contain explicit obligations on the **data processor** to ensure compliance with the Data Protection Legislation, and compliance with the rights of **Data Subjects**.

17.Images and Videos

17.1 Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR. Parents and others attending Trust events are allowed to take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child. The Trust does not prohibit this as a matter of policy.

17.2 The Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Trust to prevent.

17.3 The Trust asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

17.4 As a Trust we want to celebrate the achievements of our pupils/students and therefore may want to use images and videos of our pupils/students within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils/students, and their parents where appropriate, before allowing the use of images or videos of pupils/students for such purposes.

17.5 Precautions, as outlined in the Photography and Videos Policy, are taken when publishing photographs of pupils/students, in print, video or on the Trust/school website(s).

17.6 Whenever a pupil/student begins their attendance at the Trust they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of

images and videos of that pupil/student. We will not use images or videos of pupils/students for any purpose where we do not have consent.

18. CCTV

18.1 The Trust operates a CCTV system. Please refer to the Trust Surveillance and CCTV Policy.

19 Biometric Data

19.1 The Trust operates a Biometric recognition system for the purposes of:

- Payment of dinner monies
- Library System
- Access to electronical equipment including laptops, iPads

However, before we are able to obtain the biometric data of pupils/students or the Workforce we are required to give notification and obtain consent for this Special Category Data due to additional requirements for processing such data under the Protection of Freedoms Act 2012.

19.2 For the workforce written consent will be obtained at the commencement of their position within the Trust and shall continue to be effective unless an objection in writing to the processing of your biometric data is received from the individual.

19.3 For pupils/students under the age of 18 years, the Trust /School will notify each parent of that pupil/student (that the Trust has the contact details for and is able to contact) prior to them commencing their education at the school of the use of our Biometric Recognition System. The Trust /School will then obtain the written consent of one of the pupil/student's parent before obtaining any biometric data.

19.4 In the event that written consent cannot be obtained from a parent, or any parent objects in writing or the pupil/student objects or refuses to participate in the processing of their biometric data, the School will not process the pupil/student's biometric data and will provide the following alternative means of accessing the above services:

- providing a pin number etc as means to gain access to relevant accounts

19.5 Further information about this can be found in our Notification of Intention to Process Pupil/student's Biometric Information and our Privacy Notices.

20 Data Breach

20.1 The Trust has a Data Breach Notification Policy.

20.2 The Chief Executive Officer will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

20. DBS data

20.1 All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

20.2 Data provided by the DBS will never be duplicated.

20.3 Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

21 Policy review

21.1 This policy is reviewed annually by the Board of Trustees. However, we may change this policy at any time. Where appropriate, we will notify **data subjects** of those changes.

21.2 The next scheduled review date for this policy is September 2022.

ANNEX

DEFINITIONS

Term	Definition
Biometric Data	is information about a person's physical or behavioural characteristics or features that can be used to identify them and is obtained or recorded for the purposes of a biometric recognition system and can include fingerprints, hand shapes, features of the eye or information about a person's voice or handwriting
Biometric Recognition System	is a system that operates automatically (electronically) and : • Obtains or records information about a person's physical or behavioural characteristics or features; and • Compares or otherwise processes that information with stored information in order to establish or verify the identity of the person or otherwise determine whether they are recognised by the system
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils/students, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a 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
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our workforce (including Governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes

	personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data 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. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or Biometric Data
Workforce	Includes, any individual employed by Trust such as staff and those who volunteer in any capacity including Trustees / Members/[local governors] parent helpers