EBOR ACADEMY TRUST

Policy Number

19

GDPR Policy

Approved By:	Board of Trustees
Approval Date:	September 2020
Review Period:	Annually
Review Date:	September 2021

Author: *J Forde - School Business Manager*
Date Created/updated: *April 2020*
Version Number: *1*

Contents:

1. Introduction

1.1 Background

The General Data Protection Regulation 2016 (GDPR) replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever appropriate, that it is processed with their consent.

The provisions of the GDPR have been incorporated into the Data Protection Act (2018) ("DPA"). This incorporation creates some modification of the provisions. The DPA also offers some additional guidance in relation to the management of data protection within the education sector.

The policy is also informed by other legislation, such at the Protection of Freedoms Act of 2012 in respect of the handling of Biometric Data of persons under the age of 18.

1.2 Definitions

Material scope (Article 2) **–** the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

This definition is amended by Section 24 of the DPA which refers to manual unstructured data held by FOI public authorities. The impact of Section 24 is that manual unstructured data (that does not have to be in, or intended to be in, a filing system is subject to the provisions of Articles 15 – 19 of the GDPR

Territorial scope (Article 3) **–** the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU.

Establishment (Article 4) **–** the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal data – 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.

Special categories of personal data – 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.

Data controller – 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data Processor (Article 4) - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data subject – any living individual whose personal data is processed by or on behalf of a data controller.

Processing – 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.

Profiling **–** is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach **–** 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. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Consent **-** 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.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

1.3 Definition of a Child

The age at which a natural person is considered to be able to exercise their own rights varies in different contexts. Article 8 of the GDPR sets out that with respect to an 'Information Age Service' a person needs to be 16 years old to provide their own consent for that service to process their personal data. Member states have the option to reduce that age to 13 and the UK chose to use that option.

Under the terms of the Protection of Freedoms Act (2012) any person under the age of 18 must have the consent from a parent or guardian before their biometric data can be used. However, once parental consent has been given a person of 13 years old or above can rescind that consent.

In respect of subject access requests there are no hard age limits in England but it is presumed that a person who is 12 years old or above has the capacity to request their own personal data and by extension should be consulted if another person seeks that data.

It is our policy to recognise that the data subject has the intrinsic right to their own data and another natural person may be able to exercise the rights of the data subject depending on age or capacity.

2. Policy Statement

2.1 The Board of Directors and management of Ebor Academy Trust (the Trust), located at **[Registered Address]** are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information Ebor Academy Trust collects and processes in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act (2018).

2.2 Compliance with the GDPR is described by this policy and other relevant policies such as the Information Security Policy, the Acceptable Use Policy, along with connected processes and procedures.

2.3 The Trust is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2.4 This policy applies to all personal data processed by Ebor Academy Trust and its Trusts irrespective of the source.

2.5 Ebor Academy Trust is the data controller with responsibility for each of the Academies in the Trust. The Trust is responsible, with support from the Academies for maintaining a record of processing activities updated as appropriate when those activities change. This record will be made available to the supervisory authority upon request.

2.6 This policy applies to all Employees/Staff of L.E.A.D. Academy Trust such as outsourced suppliers. Any breach of this policy may be dealt with under Trust's disciplinary policy and may also be a criminal offence. If the Trust believes that a breach of the policy may be a criminal offence the matter will be reported as soon as possible to the appropriate authorities.

2.7 Where the Trust uses the services of a data processor it will ensure that the contract with the processor requires compliance with all the appropriate provisions of the GDPR and the DPA.

2.8 Where the Trust shares data with a third party it shall ensure that there is a lawful basis for any such sharing, that the data subjects are informed of that sharing and that the process is governed by a data sharing agreement that sets out the purposes of sharing and the steps the third party is taking to ensure that the data is processed in accordance with the GDPR and the DPA.

3. The Principles of Data Protection

3.1 This policy sets out the basis upon which the Trust processes personal data in order to be compliance with the GDPR and DPA. Article 5 of the GDPR set out the principles that any processing of personal data must abide by.

3.2 Personal data must be

3.2.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

3.2.2 Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

3.2.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

3.2.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

3.2.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 the data subject.

3.2.6 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.

3.3 This policy sets out, in Sections 4 – 11 how the Trust meets complies with the principles of data protection and the requirement for data protection by default and design. Sections 12 – 19 describe how the Trust supports the rights of data subjects. Finally Sections 20 – 29 describe how the Trust ensures the security of personal data being processed and how it deals with any failures that result in a data breach.

4. Lawful, Fair, and Transparent Data Processing

4.1 The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

4.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes;

4.1.2 The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;

4.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject;

4.1.4 The processing is necessary to protect the vital interests of the data subject or of another natural person;

4.1.5 The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

4.1.6 The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4.2 The Trust recognises that it may not use Legitimate Interest as the lawful basis for processing data associated with the performance of its public task.

4.3 If the personal data in question is "special category data" (also known as "sensitive personal data") (for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

4.3.1 The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);

4.3.2 The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);

4.3.3 The 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;

4.3.4 The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;

4.3.5 The processing relates to personal data which is clearly made public by the data subject;

4.3.6 The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

4.3.7 The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

4.3.8 The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;

4.3.9 The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

4.3.10 The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, 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.

5. Specified, Explicit, and Legitimate Purposes

5.1 The Trust collects and processes the personal data set out in Part 21 of this Policy. This includes:

5.1.1 Personal data collected directly from data subjects; and

5.1.2 Personal data obtained from third parties.

5.2 The Trust only collects, processes, and holds personal data for the specific purposes set out in Part [21] of this Policy (or for other purposes expressly permitted by the GDPR).

5.3 Data subjects are kept informed at all times of the purpose or purposes for which the Trust uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

6. Adequate, Relevant, and Limited Data Processing

6.1 The Trust and its' Academies will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 21, below.

7. Accuracy of Data and Keeping Data Updated

7.1 The Trust shall ensure that all personal data collected, processed, and held by it is kept accurate and up to date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.

7.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Data Retention

8.1 The Trust and its' Academies shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

8.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

8.3 For full details of the Trust's approach to data retention, including retention periods for specific personal data types held by the Trust and its' Academies, please refer to our Data Retention Policy, which is available on request.

9. Security of Data

9.1 The Trust shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which

shall be taken are provided in Parts 22 to 27 of this Policy.

10. Accountability and Record Keeping

10.1 The Trust's Data Protection Officer is:

10.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Trust's other data protection-related policies, and with the GDPR and other applicable data protection legislation. It shall be for the Trust and its' Academies to provide suitable records to enable this monitoring to take place.

10.3 The Trust and its' Academies shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

10.3.1 The name and details of the Trust or Academy, its Data Protection Officer, and any applicable third-party data processors;

10.3.2 The purposes for which the Trust or Academy collects, holds, and processes personal data;

10.3.3 Details of the categories of personal data collected, held, and processed by the Trust or Academy, and the categories of data subject to which that personal data relates;

10.3.4 Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

10.3.5 Details of how long personal data will be retained by the Trust or Academy (please refer to the Trust's Data Retention Policy); and

10.3.6 Detailed descriptions of all technical and organisational measures taken by the Trust or Academy to ensure the security of personal data.

10.4 The Trust as the overall data controller is required to be able to demonstrate compliance with the Data Protection Act including the elements of the GDPR contained in the Act. The Trust will demonstrate this compliance through the following documentation

10.4.1 The Record of Processing Activities for each Academy and the Trust

10.4.2 The register of data processors and associated contracts

10.4.3 A register of any data processed on behalf of other data controllers

10.4.3 A register of data sharing agreements covering disclosure to other controllers

10.4.4 A register of data breach incidents including their investigation, mitigation, communications including reporting to the regulator.

10.4.5 Data Protection Impact Assessments for all initiatives that meet the criteria

10.4.6 A record of completion of compliance activities based on best practice published by the Regulator

10.4.7 A register of audit activities, including non-compliances and actions take to mitigate that non-compliance

10.4.8 A record of the training provided to all staff.

11. Data Protection Impact Assessments

11.1 The Trust, as the overall data controller, shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.

11.2 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

11.2.1 The type(s) of personal data that will be collected, held, and processed;

11.2.2 The purpose(s) for which personal data is to be used;

11.2.3 The Trust's or Academy's objectives in bringing forward the initiative;

11.2.4 How personal data is to be used within the proposed initiative;

11.2.5 The parties (internal and/or external) who are to be consulted;

11.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

11.2.7 Risks posed to data subjects;

11.2.8 Risks posed both within and to the Trust or Academy; and

11.2.9 Proposed measures to minimise and handle identified risks.

11.3 The Trust shall have the power to delegate the compilation of a Data Protection Impact Assessment to an Academy.

12. Keeping Data Subjects Informed

12.1 The Trust shall provide the information set out in Part 12.2 to every data subject:

12.1.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

12.1.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

a) if the personal data is used to communicate with the data subject, when the first communication is made; or

b) if the personal data is to be transferred to another party, before that transfer is made; or

c) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

12.2 The following information shall be provided:

12.2.1 Details of the Trust including, but not limited to, the identity of its Data Protection Officer;

12.2.2 The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;

12.2.3 Where applicable, the legitimate interests upon which the Trust is justifying its collection and processing of the personal data;

12.2.4 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

12.2.5 Where the personal data is to be transferred to one or more third parties, details of those parties;

12.2.6 Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 28 of this Policy for further details);

12.2.7 Details of data retention;

12.2.8 Details of the data subject's rights under the GDPR and DPA;

12.2.9 Details of the data subject's right to withdraw their consent to the Trust's processing of their personal data at any time to the extent that any such consent applies;

12.2.10 Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);

12.2.11 Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

12.2.12 Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13. Data Subject Access Requests

13.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Trust holds about them, what it is doing with that personal data, and why.

13.2 Employees wishing to make a SAR should contact [INSERT DETAILS OF CONTACT POINT]

13.3 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

13.4 Responses to SARs shall be dependent upon the terms of the GDPR, the Data Protection Act (2018) and associated ICO guidance.

13.5 The Trust does not charge a fee for the handling of normal SARs. The Trust reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

14.1 Data subjects may have the right to require the Trust to rectify any of their personal data that is inaccurate or incomplete.

14.2 Where such rectification is possible, the Trust shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing

the Trust of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

14.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15. Erasure of Personal Data

15.1 Data subjects have the right to request that the Trust erases the personal data it holds about them in the following circumstances:

15.1.1 It is no longer necessary for the Trust to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

15.1.2 The data subject wishes to withdraw their consent to the Trust holding and processing their personal data;

15.1.3 The data subject objects to the Trust holding and processing their personal data (and there is no overriding legitimate interest to allow the Trust to continue doing so) (see Part 18 of this Policy for further details concerning the right to object);

15.1.4 The personal data has been processed unlawfully;

15.1.5 The personal data needs to be erased in order for the Trust to comply with a particular legal obligation; or

15.1.6 The personal data is being held and processed for the purpose of providing information society services to a child.

15.2 Unless the Trust has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

15.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of Personal Data Processing

16.1 Data subjects may request that the Trust restricts processing the personal data it holds about them. If a data subject makes such a request, the Trust shall in so far as is possible ensure that the personal data is only stored and not processed in any other fashion.

16.2 If the Trust is required to process the data for statutory purposes (as defined by purposes of processing based on the performance of a public task or substantial public interest) or for reasons of legal compliance, then the Trust shall inform the Data Subject that this processing is expected to take place. If possible, this notice will be provided prior to processing.

16.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. Data Portability

17.1 The Trust processes some personal data using automated means. Such processing is carried out by, amongst other things, our management information system(s), our human resources system and out catering management system(s).

17.2 Where data subjects have given their consent to the Trust to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Trust and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data, in a machine readable format, and to use it for other purposes (including transmitting it to other data controllers).

17.3 Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

17.4 All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

17.5 Where direct transfer to another data controller is not possible the personal data will be provided in a commonly used form such as comma separated values (.csv)

17.6 The data that can be transferred is restricted to that which has been provided by the data subject.

18. Objections to Personal Data Processing

18.1. A data subject has the right to object, on grounds relating to his or her particular situation,

to processing of personal data which is processed based on the performance of a publc task or the Legitimate Interests of the Trust.

18.2 The Trust shall no longer process the personal data unless it can demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

18.3 Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

18.4 Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

18.5 Where a data subject objects to the Trust processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the GDPR, "demonstrate grounds relating to his or her particular situation". The Trust is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

19. Automated Decision-Making

19.1 The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

19.2 The Trust may make decisions based on automated processing if that processing:

(a) is necessary for entering into, or performance of, a contract between the data subject and the Trust;

(b) is authorised by Union or Member State law to which the Trust is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

19.3 Where a data subject is unhappy with the outcome of a decision based on automated processing, the Trust with provide the opportunity for the decision to be reviewed by a person with appropriate authority to reflect the circumstances of the data

subject. The Trust's decision will be final.

19.4 The Trust will not use special category personal data to make decisions based on automated processing unless the data subject has given explicit consent or for reasons of substantial public interest. The Trust will ensure that the rights and freedoms of data subjects are safeguarded if such processing takes place.

20. Profiling

20.1 The Trust uses personal data for profiling purposes. These purposes relate to helping pupils maximise achievement and attendance.

20.2 When personal data is used for profiling purposes, the following shall apply:

20.2.1 Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;

20.2.2 The Trust will use appropriate mathematical or statistical procedures

20.2.3 The Trust will implement technical and organisational measures to minimise the risk of errors.

20.2.4 All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 to 26 of this Policy for more details on data security).

21. Personal Data Collected, Held, and Processed

21.1 The Trust uses a wide range of personal data across many processes. More detail can be found in our privacy notices. If you wish to view the complete lists of categories of personal data we process please contact our Data Protection Officer.

22. Data Security - Transferring Personal Data and Communications

22.1 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

22.2 The Trust will ensure that where special category personal data or other sensitive information is sent in the post that it shall be possible to demonstrate that it was delivered.

22.3 Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

22.4 Where special category personal data or other sensitive information is to be sent by e-mail the email will either be sent using a suitable encryption method or the data will be sent in an attached, encrypted document and not in the body of the e-mail.

22.5 Where personal data is to be transferred in removable storage devices, these devices shall be encrypted. The use of unencrypted removable storage devices is prohibited by the Trust

22.6 Where personal data is being sent by email outside of the Trust is must be secured at minimum by password protection or by the use of an appropriate encryption system.

23. Data Security - Storage

23.1 All electronic copies of personal data should be stored securely using passwords, user access rights and where appropriate data encryption;

23.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

23.3 All personal data relating to the operations of the Trust, stored electronically, should be backed up on a regular basis

23.4 Where any member of staff stores personal data on a mobile device (whether that be computer, tablet, phone or any other device) then that member of staff must abide by the Acceptable Use policy of the Trust. The member of staff shall also ensure that they can provide a secure environment for that device to be used to minimise any risk to the confidentiality or integrity of the information

24. Data Security - Disposal

24.1 When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Trust's Data Retention Policy.

25. Data Security - Use of Personal Data

25.1 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Trust requires access to any personal data that they do not already have access to, such access should be formally requested from **[Name of Authority].**

25.2 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Trust or not, without the initial authorisation of **[NAME OF PERSON]**

25.3 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time.

25.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it

25.5 Where personal data held by the Trust is used for marketing purposes, it shall be the responsibility of **[NAME OF PERSON]** to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

26. Data Security - IT Security

26.1 The Trust requires that any passwords used to access personal data shall have a minimum of [12] characters, composed of a mixture of upper and lower case characters, numbers and symbols. Passwords are not expected to be changed upon a regular basis but users will be expected to change their password if instructed by the Trust;

26.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Trust, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

26.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Trust's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and

26.4 No software may be installed on any Company-owned computer or device without the prior approval of [Name of Person].

26.5 Where members of staff or other user use online applications that require the use of personal data, the use of that application must be signed off by [Name of Person].

27. Organisational Measures

27.1 All employees, agents, contractors, or other parties working on behalf of the Trust shall be made fully aware of both their individual responsibilities and the Trust's responsibilities under the GDPR and under this Policy, and shall have free access to a copy of this Policy.

27.2 Only employees, agents, sub-contractors, or other parties working on behalf of the Trust that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Trust.

27.3 All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data will be appropriately trained to do so.

27.4 All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data will be appropriately supervised.

27.5 All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise.

27.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed.

27.7 All personal data held by the Trust shall be reviewed periodically, as set out in the Trust's Data Retention Policy.

27.8 The performance of those employees, agents, contractors, or other parties working on behalf of the Trust handling personal data shall be regularly evaluated and reviewed.

27.9 The contravention of these rules may be treated as a disciplinary matter.

27.10 All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract

27.11 All agents, contractors, or other parties working on behalf of the Trust handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of

the Trust arising out of this Policy and the GDPR

27.12 Where any agent, contractor or other party working on behalf of the Trust handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Trust against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

28. Transferring Personal Data to a Country Outside the EEA

28.1 The Trust may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

28.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

28.2.1 The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

28.2.2 The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

28.2.3 The transfer is made with the informed consent of the relevant data subject(s);

28.2.4 The transfer is necessary for the performance of a contract between the data subject and the Trust (or for pre-contractual steps taken at the request of the data subject);

28.2.5 The transfer is necessary for important public interest reasons;

28.2.6 The transfer is necessary for the conduct of legal claims;

28.2.7 The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

28.2.8 The transfer is made from a register that, under UK or EU law, is intended to provide

information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

29. Data Breach Notification

29.1 All personal data breaches must be reported immediately to the Trust's Data Protection Officer.

29.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

29.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 29.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

29.4 Data breach notifications shall include the following information:

29.4.1 The categories and approximate number of data subjects concerned.

29.4.2 The categories and approximate number of personal data records concerned.

29.4.3 The name and contact details of the Trust's data protection officer (or other contact point where more information can be obtained).

29.4.4 The likely consequences of the breach.

29.4.5 Details of the measures taken, or proposed to be taken, by the Trust to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

30. Implementation of Policy

This Policy shall be deemed effective 30th April 2020. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.