

Big Education Trust

DATA PROTECTION POLICY

1.Aims

Our trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record

3. DEFINITIONS

Personal data

Any information relating to an identified, or identifiable, living individual.

This may include the individuals:

- **name (including initials)**
- **identification number**
- **location data**
- **online identifier, such as a username**

It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special Categories of personal Data

Personal data which is more sensitive and so needs more protection, including information on racial or ethnic origin, political or religious beliefs, trade union

membership, physical and mental health, sexuality, biometric (such as fingerprints, retina and iris patterns) where used for identification purposes of genetic data and personal data relating to criminal offences and convictions.

Data Subject

An individual about whom such information is stored and processed is known as the Data Subject. It includes but is not limited to employees.

4.0 Data Controller

The organisation storing and controlling such information (i.e. the Trust) is referred to as the Data Controller. The Trust is registered with the ICO and has paid the data protection fee to the ICO, as legally required.

Processing

Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties. Processing can be automated or manual.

Automated Processing

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

Data Protection Impact Assessment (DPIA)

DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

Criminal Records Information

This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

SECTION 2 - WHEN CAN THE TRUST AND ITS SCHOOLS PROCESS PERSONAL DATA

5.0 Data Protection Principles

The Trust and its Schools are responsible for and adhere to the principles relating to the processing of personal data as set out in the GDPR.

The principles the Trust and its Schools must adhere to are: -

- (1) Personal data must be processed lawfully, fairly and in a transparent manner;

- (2) Personal data must be collected only for specified, explicit and legitimate purposes;
- (3) Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- (4) Personal data must be accurate and, where necessary, kept up to date;
- (5) Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed; and
- (6) Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Further details on each of the above principles is set out below.

Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner

The Trust and its Schools only collect, process and share personal data fairly and lawfully and for specified purposes. The Trust and its Schools must have a specified purpose for processing personal data and special category of data as set out in the GDPR.

Before the processing starts for the first time we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

Personal Data

The Trust and its Schools may only process a data subject's personal data if one of the following fair processing conditions are met: -

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- To perform a task in the public interest or in order to carry out official functions as authorised by law;
- For the purposes of the Trust and its Schools' legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

Special Category Data

The Trust and its Schools may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met: -

- The data subject has given their explicit consent;
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the The Trust and its Schools in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- Where the data has been made public by the data subject;
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- Where it is necessary for reasons of public interest in the area of public health;
- The processing is necessary for archiving, statistical or research purposes.

The Trust and its Schools identify and document the legal grounds being relied upon for each processing activity.

Consent

Where the Trust and its Schools rely on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented 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 will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

If explicit consent is required, the Trust and its Schools will normally seek another legal basis to process that data. However if explicit consent is required the data subject will be provided with full information in order to provide explicit consent.

The Trust and its Schools will keep records of consents obtained in order to demonstrate compliance with consent requirements under the GDPR.

Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes

Personal data will not be processed in any matter that is incompatible with the legitimate purposes.

The Trust and its Schools will not 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 purpose (and they have consented where necessary).

Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

The Trust and its Schools will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the The Trust and its Schools shall delete or anonymise the data. [[Please refer to the Trust and its Schools' Data Retention Policy for further guidance](#)].

Principle 4: Personal data must be accurate and, where necessary, kept up to date

The Trust and its Schools will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the Trust and its Schools.

Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The Trust and its Schools will ensure that they adhere to legal timeframes for retaining data.

We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

Please refer to the Trust and its Schools' Retention Policy for further details about how the Trust and its Schools retain and remove data.

Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

In order to assure the protection of all data being processed, the Trust and its Schools will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as: -

- Encryption;
- Pseudonymisation (this is where the The Trust and its Schools replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure);

- Ensuring authorised access (i.e. that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles;
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The Trust and its Schools follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The Trust and its Schools will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

[Full details on the Trust and its Schools' security measures are set out in [The Trust and its Schools's Security Policy.](#)]

6.0 Sharing Personal Data

The Trust and its Schools will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. These include if the third party: -

- Has a need to know the information for the purposes of providing the contracted services;
- Sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- The transfer complies with any applicable cross border transfer restrictions; and
- A fully executed written contract that contains GDPR approved third party clauses has been obtained.

There may be circumstances where the Trust and its Schools are required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities, for example, the local authority, Ofsted or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of our The Trust and its Schools shall be clearly defined within written notifications and details and basis for sharing that data given.

Transfer of Data Outside the European Economic Area (EEA)

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.

The Trust and its Schools will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the GDPR. All staff

must comply with the Trust and its Schools' guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

SECTION 3 - DATA SUBJECT'S RIGHTS AND REQUESTS

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

The rights data subjects have in relation to how the Trust and its Schools handle their personal data are set out below: -

- (a) (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;
- (b) Receive certain information about the Trust and its Schools' processing activities;
- (c) Request access to their personal data that we hold;
- (d) Prevent our use of their personal data for marketing purposes;
- (e) 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;
- (f) Restrict processing in specific circumstances;
- (g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- (h) Request a copy of an agreement under which personal data is transferred outside of the EEA;
- (i) Object to decisions based solely on automated processing;
- (j) Prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- (k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- (l) Make a complaint to the supervisory authority; and
- (m) 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.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the Trust and its Schools to verify the identity of the individual making the request.

7.0 Subject Access Requests

A Data Subject has the right to be informed by the Trust and its Schools of the following:

-

- (a) Confirmation that their data is being processed;

- (b) Access to their personal data;
- (c) A description of the information that is being processed;
- (d) The purpose for which the information is being processed;
- (e) The categories of personal data concerned
- (f) The recipients/class of recipients to whom that information is or may be disclosed;
- (g) How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- (h) Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- (i) The right to lodge a complaint with the ICO or another supervisory authority
- (j) The source of the data, if not the individual
- (k) Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- (l) The safeguards provided if the data is being transferred internationally
- (m) Details of the Trust and its Schools's sources of information obtained;
- (n) In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct.
- (o) Other supplementary information

Any Data Subject who wishes to obtain the above information must notify the Trust and its Schools in writing of his or her request. This is known as a Data Subject Access Request.

The request should in the first instance be sent to the Headteacher or equivalent.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted

without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, we:

- (a) May ask the individual to provide 2 forms of identification
- (b) May contact the individual via phone to confirm the request was made
- (c) Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- (d) Will provide the information free of charge
- (e) May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- (a) Might cause serious harm to the physical or mental health of the pupil or another individual
- (b) Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- (c) Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- (d) Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- (a) Withdraw their consent to processing at any time
- (b) Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- (c) Prevent use of their personal data for direct marketing
- (d) Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- (e) Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- (f) Be notified of a data breach (in certain circumstances)
- (g) Make a complaint to the ICO

- (h) Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

8.0 . Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils will be issued a dinner card to use at the tills.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

9.0 CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to [name/job title].

10. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

Primary students

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons.

Secondary students

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the school takes photographs and videos, uses may include:

- (a) Within school on notice boards and in school magazines, brochures, newsletters, etc.
- (b) Outside of school by external agencies such as the school photographer, newspapers, campaigns
- (c) Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Direct Marketing

The Trust and its Schools are subject to certain rules and privacy laws when marketing. For example a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

The Trust and its Schools will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The Trust and its Schools will promptly respond to any individual objection to direct marketing.

Employee Obligations

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the Trust and its Schools in the course of their employment or engagement. If so, the Trust and its Schools expect those employees to help meet the Trust and its Schools' data protection obligations to those individuals. Specifically, you must: -

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure (for example by complying with rules on access to the Trust and its Schools' premises, computer access, password protection and secure file storage and destruction [[Please refer to the Trust and its Schools's Security Policy for further details about our security processes](#)]);
- Not to remove personal data or devices containing personal data from the Trust and its Schools premises unless appropriate security measures are in place (such as Pseudonymisation, encryption, password protection) to secure the information;
- Not to store personal information on local drives.

SECTION 4 - ACCOUNTABILITY

The Trust and its Schools will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the GDPR principles.

The Trust and its Schools have taken the following steps to ensure and document GDPR compliance: -

Data Protection Officer (DPO)

Please find below details of the The Trust and its Schools's Data Protection Officer: -

Data Protection Officer: Craig Stilwell
Address: Judicium Consulting Ltd, 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Telephone: 0203 326 9174

The DPO is responsible for overseeing this data protection policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances: -

- (a) If you are unsure of the lawful basis being relied on by the Trust and its Schools to process personal data;
- (b) If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);
- (c) If you need to draft privacy notices or fair processing notices;

- (d) If you are unsure about the retention periods for the personal data being processed [[but would refer you to the Trust and its Schools' data retention policy in the first instance](#)];
- (e) If you are unsure about what security measures need to be put in place to protect personal data;
- (f) If there has been a personal data breach [[and would refer you to the procedure set out in the Trust and its Schools' breach notification policy](#)];
- (g) If you are unsure on what basis to transfer personal data outside the EEA;
- (h) If you need any assistance dealing with any rights invoked by a data subject;
- (i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;
- (j) If you plan to undertake any activities involving automated processing or automated decision making;
- (k) If you need help complying with applicable law when carrying out direct marketing activities;
- (l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

Personal Data Breaches

The GDPR requires the Trust and its Schools to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

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.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the key point of contact for personal data breaches (who is Michele Barthram) or your DPO.

Transparency and Privacy Notices

The Trust and its Schools will provide detailed, specific information to data subjects. This information will be provided through the Trust and its Schools' privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. Privacy notices set out information for data subjects about how the Trust and its Schools use their data and the Trust and its Schools' privacy notices are tailored to suit the data subject.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the GDPR including the identity of the data protection officer, the Trust and its Schools' contact details, how and why we will use, process, disclose, protect and retain personal data.

When personal data is collected indirectly (for example from a third party or publically available source), we will provide the data subject with the above information as soon as possible after receiving the data. The Trust and its Schools will also confirm whether that third party has collected and processed data in accordance with the GDPR.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as “children” under the GDPR

Privacy by Design

The Trust and its Schools adopt a privacy by design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the Trust and its Schools take into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

Data Protection Impact Assessments (DPIAs)

In order to achieve a privacy by design approach, the Trust and its Schools conduct DPIAs for any new technologies or programmes being used by the Trust and its Schools which could affect the processing of personal data. In any event the Trust and its Schools carry out DPIAs when required by the GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large scale processing of special category data;
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Our DPIAs contain: -

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

Record Keeping

The Trust and its Schools are required to keep full and accurate records of our data processing activities. These records include: -

- The name and contact details of the Trust and its Schools;
- The name and contact details of the Data Protection Officer;
- Descriptions of the types of personal data used;
- Description of the data subjects;
- Details of the Trust and its Schools’ processing activities and purposes;
- Details of any third party recipients of the personal data;
- Where personal data is stored;
- Retention periods; and
- Security measures in place.

Training

The Trust and its Schools will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

Audit

The Trust and its Schools through its data protection officer regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place annually in order to review use of personal data.

Related Policies

Staff should refer to the following policies that are related to this data protection policy:

-

- Data retention policy;
- Data breach policy;
- Security policy.

These policies are also designed to protect personal data and can be found by contacting the school.

SECTION 5 - AUTOMATED PROCESSING AND AUTOMATED DECISION MAKING

Generally automated decision making is prohibited when a decision has a legal or similar significant effect on an individual unless:

- (a) The data subject has given explicit consent;
- (b) The processing is authorised by law; or
- (c) The processing is necessary for the performance of or entering into a contract.

If certain types of sensitive data are being processed, then (b) or (c) above will not be allowed unless it is necessary for the substantial public interest (for example fraud prevention).

If a decision is to be based solely on automated processing, then data subjects must be informed of their right to object. This right will be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the data subject's rights and freedoms and legitimate interests.

The Trust and its Schools will also inform the data subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the data subject the right to request human intervention, express their point of view or challenge the decision.

The Trust and its Schools will carry out a data protection impact assessment before any automated processing or automated decision making activities are undertaken.

Monitoring

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the Trust and its Schools.