DIOCESE OF CHICHESTER ACADEMY TRUST

St Joseph's Junior St Joseph's Nursery and Infant school

DATA PROTECTION POLICY

Date Agreed:	**June 2021**
Review Date:	**June 2023**
Type of Policy:	**DCAT Statutory Policy**

Revision Number	Date Issued	Prepared by	Approved	Personalised by school	Comments
4	June 2021	DCAT	Trust Board		DPO
3	June 2020	CF			DPO
2	May 2018	SJP/DC			JUDICIUM
1	May 2017	SJP	DCAT Directors		

Type of Policy	*Tick* ✓
DCAT Statutory Policy	✓
DCAT Non-statutory Policy	
DCAT Model Optional Policy	
School Policy	
Local Authority Policy	

Contents

Introduction

Our **vision** for our Trust is we exist to:

Help every child achieve their God-given potential

Our **aims** are clear. We aim to be a Trust in which:

Developing the whole child means pupils achieve and maximise their potential

Continued development of staff is valued and improves education for young people

All schools are improving and perform above national expectations

The distinct Christian identity of each academy develops and is celebrated

Our work as a Trust is underpinned by shared **values**. They are taken from the Church of England's vision for Education and guide the work of Trust Centre team. They are:

Aspiration
I can do all things through Christ who strengthens me
(Philippians 4 vs 13).

Wisdom
Listen to advice and accept discipline, and at the end you will be counted among the wise
(Proverbs 19 vs 20)

Respect
So in everything do to others what you would have them do to you
(Matthew 7 vs 12)

Our vision of helping every child achieve their God-given potential is aligned with the Church of England's vision for education and is underpinned by the Bible verse from John: *I have come that they may have life, and have it to the full.*

1. Policy Aims

The General Data Protection Regulation (GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The Trust will protect and maintain a balance between data protection rights in accordance with the GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers, volunteers and other third parties.

This policy does not form part of any individual's terms and conditions of employment with the Trust and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Trust's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy sets the Trust's obligations regarding the collection, processing, transfer, storage and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Trust, its employees, agents, volunteers, contractors or other parties working on behalf of the Trust.

The Trust is not only committed 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.

The Trust is the registered Data Controller, however, most information will be stored at School level and therefore the terms "Trust" and "School" should be interchangeable throughout this policy.

2. Definitions

2.1 Personal data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

2.2 Special Category Data

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

2.3 Data Subject

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

2.4 Data Controller

The organisation storing and controlling such information (i.e. the Trust) is referred to as the Data Controller.

2.5 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.

2.6 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.

2.7 Data Protection Impact Assessment (DPIA)

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

2.8 Criminal Records Information

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

3. When can the Trust/School Process Personal Data

3.1 Data Protection Principles

The Trust is responsible for adhering to the principles relating to the processing of personal data as set out in the GDPR. The Trust aims to ensure compliance with the Act including the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply.

The principles the Trust 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 and not further processed in a manner that is incompatible with those 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. 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;

(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 School/Trust only collects, processes and shares personal data fairly and lawfully and for specified purposes. The School/Trust 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).

<u>Personal Data</u>

The School/Trust may only process a data subject's personal data if one of the following fair processing conditions is 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's 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 School/Trust 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 School/Trust 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 in necessary for archiving, statistical or research purposes.

The School/Trust identifies and documents the legal grounds being relied upon for each processing activity.

Consent

Where the School/Trust relies 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 the 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 School/Trust 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 School/Trust 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 School/Trust 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 School/Trust will only process personal data when our obligations and duties require us to. We will not collect any more data than is necessary and we will ensure that any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the School/Trust shall delete or anonymise the data. Please refer to the Trust's Data Retention Policy for further guidance.

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

The School/Trust 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 School/Trust.

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 School/Trust will ensure that it adheres 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's Retention Policy for further details about how the School/Trust retains and removes 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 School/Trust will develop, implement and maintain reasonable safeguard and security measures. These include using measures such as: -

- Encryption;
- Pseudonymisation (this is where the School/Trust 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 School/Trust follows procedures and uses technologies to ensure security; and it will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data. The School/Trust 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.

3.2 Sharing Personal Data

The School/Trust 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 School/Trust is required either by law or in the best interests of our pupils, parents or staff to pass information to external authorities, for example, the local authority, Ofsted or the department of health. These authorities comply 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 our School/Trust shall be clearly defined in written notifications which include the details and the basis for sharing that data.

3.3 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 School/Trust 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's 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.

4. Data Subject's Rights and Requests (SAR)

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 School/Trust handles their personal data are: -

(a) (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;

(b) To receive certain information about the School's/Trust's processing activities;

(c) To request access to their personal data that we hold;

(d) To prevent our use of their personal data for marketing purposes;

(e) To 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) To restrict processing in specific circumstances;

(g) To challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) To request a copy of an agreement under which personal data is transferred outside of the EEA;

(i) To object to decisions based solely on automated processing;

(j) To prevent processing that is likely to cause damage or distress to the data subject or anyone else;

(k) To be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

(l) To make a complaint to the supervisory authority; and

(m) In limited circumstances, to receive or to 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 School/Trust to verify the identity of the individual making the request.

4.1 Subject Access Requests

A Data Subject has the right to be informed by the School/Trust 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 recipients/class of recipients to whom that information is to be or may be disclosed;

(f) Details of the School's/Trust's sources of information obtained;

(g) 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 them, to be informed of the reasons for the Data Controller's decisions. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct.

(h) Other supplementary information

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

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

The School/Trust has defined a process for handling SARs and other data subject requests. This process is mandatory for all staff.

Any Data Subject who wishes to obtain the above information must notify the Trust in writing of their request. This is known as a Data Subject Access Request.

The request should in the first instance be sent to the school. The Subject Access Request (SAR) form can be found here. When the school receives the request, they need to notify the DPO using a notification of a SAR form and acknowledge receipt of the SAR. The SAR will be given a unique reference number (URN) so this can be logged.

4.2 Direct Marketing

The Trust is 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 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 will promptly respond to any individual objection to direct marketing.

4.3 Employee Obligations

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the School/Trust in the course of their employment or engagement. If so, the School/Trust expects those employees to comply with the School's/Trust's data protection obligations to those individuals. Specifically, employees accessing the personal data of staff, suppliers, parents or pupils must: -

- Only access the personal data they 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 School/Trust premises, computer access, password protection and secure file storage and destruction;
- Not to remove personal data or devices containing personal data from the School/Trust 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.

4.4 Automated Decision Making

Data subjects have the right not to be subject to a decision based on automated processing of their personal data, including profiling, where that decision has a legal effect or significantly affects them.

The School/Trust may use such processing if the decision:

- Is necessary for entering into, or for managing the performance of, a contract between the data subject and a data controller;
- Is authorised by a Union or Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- Is based on the data subject's explicit consent.

Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge to such decisions under the GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the School/Trust.

Such decisions should not concern a child (natural persons under the age of 18) unless there is a compelling, demonstrated and documented reason for doing so.

5. Accountability

The School/Trust 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 have taken the following steps to ensure and document GDPR compliance.

5.1 Data Protection Officer (DPO)

Please find below details of the Trust's Data Protection Officer: -
Data Protection Officer: Jo Saunders
Address: DCAT, St Catherine's College, Priory Road, Eastbourne BN23 7BL
Email: dpo@dcat.academy
Telephone: 01273 056292

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 School/Trust 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 School's/Trust's 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 School's/Trust's 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.

5.2 Personal Data Breaches

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

All personal data breaches must be reported immediately to the person responsible for GDPR at the School who will in turn report to the Trust DPO.

If a personal data breach occurs and that data 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 ICO is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk (higher than those mentioned above) to the rights and freedoms of data subjects, the DPO must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include, a minimum, the following information:

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of the School's/Trust's DPO (or other contact point where more information can be obtained)
- The likely consequences of the breach;
- Details of the measures taken, or proposed to be taken, by the School/Trust to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

The Trust has a detailed policy for managing personal data breaches which can be found here.

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 DPO.

5.3 Transparency and Privacy Notices

The School/Trust will provide detailed, specific information to data subjects. This information will be provided through the School's/Trust's 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 sets out information for data subjects about how the School/Trust use their data and the School's/Trust's 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 School's/Trust's 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 from a publicly available source), we will provide the data subject with the above information as soon as possible after receiving the data. The School/Trust 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.

5.4 Privacy by Design

The School/Trust 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 School/Trust takes 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.

5.5 Data Protection Impact Assessments (DPIAs)

In order to achieve a privacy by design approach, the School/Trust conducts DPIAs for any new technologies or programmes being used by the School/Trust which could affect the processing of personal data. In any event the School/Trust carries 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.

DPIAs shall be overseen by the DPO and shall address the following:

- The type(s) of personal data that will be collected, held and processed:
- The purpose(s) for which personal data is to be used:
- The School's/Trust's objectives:
- How personal data is to be used:
- The parties (internal/external) who are to be consulted:
- The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed:
- Risks posed to data subjects:
- Risks posed both within and to the School/Trust; and
- Proposed measures to minimise and handle identified risks.

5.6 Accountability & Record Keeping

Each School has a designated person responsible for GDPR. The Trust DPO is the GDPR lead and responsible for overseeing this policy and for monitoring compliance with this Policy, the School's/Trust's other data protection protection-related policies and with the GDPR and other applicable data legislation.

Each School is required to keep full and accurate records of our data processing activities. These records include: -

- The name and contact details of the School and the person designated as responsible for GDPR in the school;
- 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 School's 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.
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards.
- The purpose for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing
- Where applicable, the legitimate interests upon which the School/Trust is justifying its collection and processing of the personal data
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

- Where the personal data is to be transferred to a third party that is located outside the EEA, details of that transfer, including but not limited to, the safeguards in place
- Details of data retention
- Details of the subject's data rights under the GDPR
- Details of the data subject's right to withdraw their consent to the School's/Trust's processing of their personal data at any time;
- Details of the data subject's right to complain to the ICO
- 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
- 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.

5.7 Organisational Measures and Training

The School/Trust will ensure that the following measures are taken with respect to the collection, holding and processing of personal data.

- All employees, agents, volunteers, contractors or other third parties working on behalf of the School/Trust shall be made fully aware of both their individual responsibilities and the School/Trust responsibilities under the GDPR and under this Policy, and shall have free access to a copy of this policy.
- Only employees, agents, volunteers, sub-contractors, or other third parties working on behalf of the School/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 School/Trust.
- All employees, agents, volunteers, sub-contractors or other third parties working on behalf of the School/Trust handling personal data will be appropriately trained to do so
- All employees, agents, volunteers, sub-contractors or other third parties working on behalf of the School/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;
- All employees, agents, volunteers, sub-contractors or other third parties working on behalf of the School/Trust handling personal data must ensure that any and all of their employees working on behalf of the School/Trust handling personal data will be bound to do so in accordance with the principles of the GDPR and this policy by contract.
- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;
- All personal data held by the School/Trust shall be reviewed periodically, as set out in the School's/Trust's Data Retention Policy;
- The performance of those employees, agents, volunteers, contractors, or other third parties working on behalf of the School/Trust handling personal data shall be regularly evaluated and reviewed;
- The contravention of these rules will be treated as a disciplinary matter;
- All employees, agents, volunteers, sub-contractors or other third parties 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 School/Trust arising out of this policy and the GDPR; and,

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

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

5.8 Audit

The Trust, through the DPO, will 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.

5.9 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 School/Trust.

6. Data Security

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

The School/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.

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.

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 School/Trust.

6.1 Data security – Storage

The School/Trust shall ensure that the following measures are taken with respect to the storage of personal data:

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

- 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:
- All personal data relating to the operations of the School/Trust, stored electronically, should be backed up on a regular basis
- 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 School/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.

6.2 Data security – IT security

Full details of the School's/Trust's IT security requirements and procedures can be found in the IT Security Policy. The School/Trust shall ensure that, inter alia, the following measures are taken with respect to IT and information security:

The School/Trust requires that any passwords used to access personal data shall have a minimum of 6characters, 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 School/Trust:

Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the School/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:

All software (including, but not limited to, applications and operating systems) shall be kept up to date. The School's/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

No software may be installed on any School/Trust-owned computer or device without the prior approval of JSPC

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 JSPC.

7. Related Policies

Staff should refer to the following policies that are related to this Data Protection Policy.

- Electronic Information and Communications Systems Policy
- Data Breach Policy
- Data Retention Policy
- CCTV Policy
- Information Security Policy

- Freedom of Information Policy
- Privacy Notices

These policies are also designed to protect personal data and can be found here.