Data Protection Policy

Date reviewed: October 2024

Next review by: October 2025

Person Responsible: Chief Operating Officer

Contents

1. AIMS & INTRODUCTION

5 Dimensions Trust collects and uses certain types of personal information about staff, students, parents/ guardians and other individuals who come into contact with the Trust in order to provide education and associated functions.

We aim to ensure that all personal data collected about staff, students, parents, guardians, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

The Trust may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation (GDPR) and other related legislation.

The Trust informs individuals of the type of data we process and what we do with this information through our privacy notices that can be found here: 5 Dimensions Trust

The GDPR apply to all computerised data and physical files

2. LEGISLATION AND GUIDANCE

This policy meets the requirements of the:

UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

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 our funding agreement and articles of association.

3. DEFINITIONS

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: › 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 about an individual's: › Racial or ethnic origin › Political opinions › Religious or philosophical beliefs › Trade union membership › Genetics › Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes › Health – physical or mental › Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. THE DATA CONTROLLER

The Trust processes personal data relating to parents, students, staff, trustees, governors, visitors, and others, and therefore is a data controller. The school is registered with the ICO, as legally required.

5. ROLES AND RESPONSIBILITIES

This policy applies to **all staff** employed by our Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing body

The governing body has overall responsibility for ensuring that our Trust complies with all relevant data protection obligations.

Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the board of trustees and local governing bodies and, where relevant, report to the body their advice and recommendations on school data protection issues.

The Data Protection Officer is also the first point of contact for individuals whose data the Trust processes, and for the ICO. (Information Commissioners Office). The Data Protection Officer for 5 Dimensions Trust is Mrs J Strong. The Data Protection Lead has day-to-day responsibility for data protection issues in our Trust / school. The Data Protection Lead is Ms H Carty.

Full details of the Data Protection Officer's responsibilities are set out in their job description.

The School / Academy specific GDPR Data Protection Leads are:

- The Hazeley Academy — Lindsey Soper
- Shenley Brook End School — Gareth McCluskey
- Priory Rise School — Corinne Benham-Smith

Headteacher / Principal

The headteacher / principal of each school / academy acts as the representative of the data controller on a day-to-day basis.

All staff

Staff are responsible for:

- Collecting, storing, and processing any personal data in accordance with this policy
- Informing the Trust of any changes to their personal data, such as a change of address

› Contacting the Data Protection Officer in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
- If they have any concerns that this policy is not being followed.
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK.
- If there has been a data breach.
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
- If they need help with any contracts or sharing personal data with third parties.

6. THE DATA PROTECTION PRINCIPLES.

The UK GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant, and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the school aims to comply with these principles.

7. COLLECTING PERSIONAL DATA

Lawfulness, fairness and transparency

We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can **perform a task in the public interest or exercise its official authority**

- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent**

For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a student) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a student) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

8. USE OF PERSONAL DATA BY THE TRUST

The Trust holds personal data on students, staff, and other individuals such as visitors. In each case,the personal data must be treated in accordance with the data protection principles and collected as outlined in the 5 Dimensions Trust privacy notices.

Students

The personal data held regarding students includes, but is not limited to, contact details, assessment, examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information and photographs.

The data is used in order to support the education of the students, to monitor and report on their progress, to provide appropriate pastoral care and to assess how well the Trust as a whole is doing, together with any other uses normally associated with this provision in a school /academy environment.

In particular, the Trust may:

- Make personal data, including sensitive personal data, available to staff for planning curricular orextra-curricular activities.
- Keep the student's previous school informed of his/her academic progress and achievements e.g.,sending a copy of the school reports for the student's first year at the School / Academy to the previous school.
- Use of photographs of students for internal identification and/or advertising

Staff

The personal data held about staff will include, but is not limited to, contact details, employment history, information relating to their career progression, information relating to DBS checks, photographs, training records, emergency contact details, sickness records including medical certificates.

The data is used to comply with legal obligations placed on the school / academy in relation to employment and the education of children.

The Trust may pass information to other regulatory authorities where appropriate and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.

Staff should note that information about disciplinary action may be kept longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

Other Individuals

The Trust may hold personal information in relation to other individuals who have contact with the school / academy, such as volunteers, guests and parents or guardians of students. Such information shall be held only in accordance with the data protection principles and shall not be kept longer than necessary.

Right to limit or object

Any wish to limit or object to the uses to which personal data is to be put should be notified to the school / academy specific GDPR Data Protection Lead (listed at the end of this policy), who will ensure that it is recorded and adhered to if appropriate. If the GDPR Data Protection Lead is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why the Trust cannot comply with their request.

9. SECURITY OF PERSONAL DATA

The Trust will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this policy and their duties under the GDPR. The Trust will take all reasonable steps to ensure that all personal information is held securelyand is not accessible to unauthorised persons.

10. DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES

The following list includes the most usual reasons that the Trust will authorise disclosure of personal data to a third party:

- To give a confidential reference relating to a current or former employee, volunteer or student.
- For the prevention or detection of crime.
- For the assessment of any tax or duty.
- Where it is necessary to exercise a right or obligation conferred or imposed by law upon the Trust (other than an obligation by contract).
- For the purpose of, or in connection with legal proceedings (including prospective legal proceedings).
- For the purpose of obtaining legal advice.
- For research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress).
- To publish the results of public examinations or other achievements of students of the Trust.
- To disclose details of a student's medical condition where it is in the student's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips.
- To provide information to another educational establishment to which a student is transferring
- To provide information to the Examination Authority as part of the examination process
- To provide information to the relevant Government Department concerned with national education. At the time of writing this policy this department is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

The DfE uses information about students for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual students cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.

The Trust may receive requests from third parties (i.e. those other than the data subject, the Trust and employees of the Trust) to disclose personal data it holds about students, their guardians or parents, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosures apply, or where necessary for the legitimate interests of the Trust.

All requests for the disclosure of personal data must be sent to the GDPR Data Protection Lead, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third person before making any disclosure.

11. CONFIDENTIALITY OF PUPIL/STUDENT CONCERNS

Where a student seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, the Trust will maintain confidentiality unless it has reasonable grounds to believe that the student does not fully understand the consequences of withholding their consent or where the Trust believes disclosure will be in the best interests of the student or other students.

Child protection and safeguarding take precedence in all areas around confidentiality of student concerns.

12. EXEMPTIONS TO ACCESS BY DATA SUBJECTS

Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

There are other exemptions from the right of subject access. If we intend to apply any of them to a request, then we will usually explain which exemption is being applied and why.

13. PERSONAL ELECTRONIC DEVICES

Where necessary for the execution of its' responsibilities under legislation the Trust may obtain data from personal electronic devices. The member of staff obtaining the data will ensure that they explain the reasons why they are taking the data and that it will be stored securely in a limited and protected area. Access will be limited to those who need it to fulfil their roles and responsibilities and storage and disposal will occur as per the rest of the policy. Requests for access to this data are explained earlier in this policy.

Images will be stored on a secure server with limited and protected access for those who need it to fulfil their roles and responsibilities. Where this data is used for the purposes outlined above, storage and disposal will occur as per the rest of the policy.

14. BREACH OF ANY REQUIREMENT OF THE GDPR

All breaches of the GDPR, including a breach of any of the data protection principles, shall be reported as soon as it is discovered to the GDPR Data Protection Lead.

Once notified, the GDPR Data Protection Lead will assess in conjunction with the Data Protection Officer.

- The extent of the breach.
- The risks to the data subjects as a consequence of the breach.

- Any security measures in place that will protect the information.
- Any measures that can be taken immediately to mitigate the risk to the individuals.

Unless the GDPR Data Protection Lead and Data Protection Officer concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office with 72 hours of the breach having come to the attention of the Trust, unless a delay can be justified. The Information Commissioner shall be told:

- Details of the breach, including the volume of the data at risk and the number and categories of data subjects.
- The contact point for any enquiries, which will normally be the Data Protection Officer.
- The likely consequence of the breach.
- The measures proposed or already taken to address the breach.

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals, then the GDPR Data Protection Lead shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

Data subjects shall be told:

- The nature of the breach.
- Who to contact with any questions.
- Measures taken to mitigate any risks.

The Data Protection Officer shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the Trust and a decision made about implementations of these recommendations.

If the breach is not likely to present a risk to individuals, the same processes shall apply, but an internal record shall be kept instead.

15. SHARING PERSONAL DATA

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a student or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law.
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share.

- Only share data that the supplier or contractor needs to carry out their service.

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

16. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing.
- The right to lodge a complaint with the ICO or another supervisory authority.
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.
- The safeguards provided if the data is being transferred internationally.

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual.
- Correspondence address.
- Contact number and email address.
- Details of the information requested.

If staff receive a subject access request in any form they must immediately forward it to the DPO.

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 students at our school may be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

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 students at our school may not be granted without the express permission of the student. This is not a rule and a student'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:

- May ask the individual to provide 2 forms of identification.
- May contact the individual via phone to confirm the request was made.
- 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).
- Will provide the information free of charge.
- 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:

- Might cause serious harm to the physical or mental health of the student or another individual.
- 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.
- 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.
- 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:

- Withdraw their consent to processing at any time.
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances).
- Prevent use of their personal data for direct marketing.

- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests.
- 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).
- Be notified of a data breach (in certain circumstances).
- Make a complaint to the ICO.
- 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.

17. PARENTAL REQUESTS TO SEE THE EDUCATION RECORD

The 5 Dimensions Trust 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. Requests should be made directly to the school.

18. BIOMETRIC RECOGNITION SYSTEMS

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive school / academy 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 Trust 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 students have the right to choose not to use the Trusts' biometric system(s).

Parents/carers and students 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 student 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 student's parent(s)/carer(s).

Where staff members or other adults use the school's / academy'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 Trust will delete any relevant data already captured.

19. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

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 the Headteacher.

Purpose

The purpose is to regulate the management, operation and use of the closed-circuit television system for the schools / academies within the 5 Dimensions Trust. The systems are owned and operated by the school / academy and comprises several cameras located in and around the school / academy sites.

The CCTV system and use of all information, documents and recordings comply with all legal requirements. The CCTV system is to

- protect the security of the school building, car parks, other public areas, and assets.
- increase the personal safety of students, staff, and visitors.
- assist in managing the school.
- support the Police in a bid to deter and detect crime.

Responsible Person

The IT department have been appointed to oversee the system and procedures.

Quality Control

A regular maintenance programme is in place. A check to ensure the equipment is properly recording, that cameras are functional, the quality of images being collected is good and the date and time accurate will be carried out as required. During times of school / academy closure, the CCTV system will continue to operate as normal.

Retention of Images

Images are retained for 31 days after which they are overwritten or in the event of a recorded incident, retained for evidential purposes until no longer required.

Access

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Access to live and recorded images are managed by software user access rights.

Access to view live images is restricted to:

- Members of the leadership group.
- Year Leaders.
- Sixth Form and Attendance Staff.
- IT Network Manager (or other delegated person in their absence).
- Delegated staff by the headteacher to investigate an incident.

Access to view live and recorded images is restricted to:

- Members of the leadership group.
- Year Leaders.
- Sixth Form and Attendance Staff.
- IT Network Manager (or other delegated person in their absence).
- Delegated staff by the headteacher to investigate an incident.

Access to view recorded images is restricted to:

- Governors
- Appropriate people involved in investigations where recorded images are required to be considered.

Images may be viewed and copied for the Police for the prevention and detection of crime. Should any images be required by the Police, we will:

- record the date and time of the request and the image
- record the name and rank of the requesting officer.

All requests to view images should be made in writing and will only be released with the approval of the responsible person. Applications received from outside bodies (eg solicitors) to view or release images will be referred to the responsible person. In these circumstances images will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. A fee will be charged in such circumstances. Images will only be released to the media for use in the investigation of a specific crime and with the written authority of the Police.

Images will never be released to the media for the purposes of entertainment. Images will be viewed in an appropriate area where they cannot be accidentally viewed by others.

A log of disclosure will be kept by the responsible person.

20. PHOTOGRAPHS AND VIDEOS

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

Primary

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 the student.

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 students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Secondary

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students 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 the student. Where we don't need parental consent, we will clearly explain to the student 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 students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or students where appropriate) have agreed to this.

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

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns

- 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.

21. ARTIFICIAL INTELLIGENCE (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. 5 Dimensions Trust recognises that AI has many uses to help students learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, 5 Dimensions Trust will treat this as a data breach, and will follow the personal data breach procedure outlined in this policy.

22. DATA PROTECTION BY DESIGN AND DEFAULT

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO, and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

23. DATA SECURITY AND STORAGE OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access.
- Where it is necessary for information to be taken off site, staff are provided training on how to protect data and avoid potential breaches.
- Passwords that are at least 7 characters long containing letters and numbers and including one capital letter are used to access school computers, laptops and other electronic devices. Staff and students are reminded that they should not reuse passwords from other sites.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment see our ICT Acceptable Use Policy.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

24. DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

25. PERSONAL DATA BREACHES

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in this policy.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website, which shows the exam results of students eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about students.

26. TRAINING

All staff and governors are provided with data protection training as part of their induction process and is renewed annually.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

27. MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing this policy.

This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation and shall be reviewed every year.

28. LINKS WITH OTHER POLICIES

This data protection policy is linked to our:

- Data Retention Schedule.
- Privacy notices.
- ICT Acceptable Use Policy.

29. PERSONAL DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by email.
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- Staff, trustees, and governors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher and the chair of governors/trustees.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure).
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences.

- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool.
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Trust's computer systems.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned.
        - The categories and approximate number of personal data records concerned.
    - The name and contact details of the DPO.
    - A description of the likely consequences of the personal data breach.
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach.
    - The name and contact details of the DPO.
    - A description of the likely consequences of the personal data breach.
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the Trust's computer systems.

The DPO and headteacher/principal/data protection leads will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

The DPO and headteacher/principal/data protection leads will meet as required to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Example of relevant actions: **Sensitive information being disclosed via email (including safeguarding records)**

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners