# Data Protection and Freedom of Information Policy

Date Ratified: 30th September 2021
Person responsible : Principal

## 1. AIMS & INTRODUCTION.

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

**Five Dimensions Trust is the Governing body for Shenley Brook End School and The Hazeley Academy. This policy is intended to be used by the Trust for these and any additional schools / academies that may join the Trust.**
**The policy will be updated to reflect any changes as soon as reasonably possible.**

Five 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 intendedto 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 thisinformation through our privacy notices that can be found here: 5 Dimensions Trust

The GDPR apply to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way thatit is searchable on the basis of specific criteria (so you would be able to use an individual's name tofind their information), and if this is the case, it does not matter whether the information is locatedin a different location.

This policy will be updated as necessary to reflect best practice, or amendments made to dataprotection legislation and shall be reviewed every 2 years.

## 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 GDPR.

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

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

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

## 3. DEFINITIONS

| TERM | DEFINITION |
|---|---|
| **Personal data** | Any information relating to an identified, or identifiable, living individual.<br>This may include the individual's:<br>› Name (including initials)<br>› Identification number<br>› Location data<br>› Online identifier, such as a username<br>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:<br>› Racial or ethnic origin<br>› Political opinions<br>› Religious or philosophical beliefs<br>› Trade union membership<br>› Genetics<br>› Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>› Health – physical or mental<br>› 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.<br>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, pupils, staff, 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.

### 5.1 Governing body

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

### 5.2 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 governing body 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).

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

Our Data Protection Officer and Data Protection Leads are named in appendix 7.1.

### 5.3 Headteacher / Principal

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

### 5.4 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

### 5.5 Individual personal data

Personal data is information that identifies an individual and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain.

Special Category Information is given special protection and additional safeguards apply if this information is to be collected and used.

Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

The Trust does not intend to seek or hold sensitive personal data about staff or students except where the Trust has been notified of the information, or it comes to the Trust's attention via legitimate means e.g. a grievance or needs to be sought and held in compliance with a legal obligationor as a matter of good practice. Staff or students are under no obligation to disclose to the Trust their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / orparenthood are needed for other purposes, e.g., pension entitlements).

The Trust is the data controller for the purposes of the Data Protection act 2018 and isregistered with the Information Commissioner's Office

Personal data should always be kept securely and protected by passwords if it is electronic; access should only be those authorised to see it – confidentiality should be respected. The law also provides that personal data should not be kept longer than is required.

## 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

The six data protection principles as laid down in the GDPR are followed at all times:

- Personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met.

- Personal data shall be collected for specific, explicit, and legitimate purposes and shall not be further processed in a manner incompatible with those purposes.
- Personal data shall be adequate, relevant, and limited to what is necessary for the purpose forwhich it is being processed.
- Personal data shall be accurate and where necessary, kept up to date.
- Personal data processed for any purpose (s) shall not be kept for longer than is necessary for that purpose / those purposes.
- Personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

In addition to this, the Trust is committed to ensuring at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law

The Trust is committed to complying with the principles (6) at all times. This means the trust will:

- Inform individuals as to the purpose of collecting any information from them, as and whenwe ask for it.
- Be responsible for checking the quality and accuracy of the information.
- Regularly review the record held to ensure that information is not held longer than is necessary and that it has been held in accordance with statutory and best practice for data retention
- Ensure that when information is authorised for disposal it is done appropriately.
- Ensure appropriate security measures to safeguard personal information whether it is heldin paper files or on our computer systems
- Share personal information with others only when it is necessary and legally appropriate todo so.
- Set out clear procedures for responding to requests for access to personal informationknown as subject access requests.
- Report any breaches of the GDPR in accordance with procedures stated in section 12.

## 7. CONDITIONS FOR THE PROCESSING IN THE FIRST DATA PRINCIPLE.

One or more of the following conditions must be met in order to process data.

A register of processing activities and conditions met will be maintained by the School / Academy along with an asset register of the systems used.

- The individual has given consent that is specific to the particular type of processing activity and that consent is informed, unambiguous and freely given.
- The process is necessary for the performance of a contract, to which the individual is a party, oris necessary for the purpose of talking steps with regards to entering into a contract with the individual at their request.
- The processing is necessary for the performance of a legal obligation to which we are subject. The processing is necessary to protect the vital interests of the individual or another.
- The processing is necessary for the performance of a task carried out in the public interest, or inthe exercise of official authority vested in us.
- The processing is necessary for a legitimate interest of the School / Academy or that of a third party, exceptwhere this interest is overridden by the rights and freedoms of the individual corned.

## 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 as outlined in Section 3.

### 8.1 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 in accordance with the photograph policy.

### 8.2 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 in relation to employment and the education of Children in a school / academy environment.

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.

### 8.3 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.

### 8.4 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 in Appendices), 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 datain 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.

For further details as regards security of IT systems, please refer to the school / academy specific ICT procedures.

## 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 pupil.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 theTrust (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 pupils of theTrust.
- To disclose details of a pupil's medical condition where it is in the pupil'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 pupil is transferring
- To provide information to the Examination Authority as part of the examination process: and
- 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 pupils 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 pupils 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, theTrust and employees of the Trust) to disclose personal data it holds about pupils, 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 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 pupil does not fully understand the consequences of withholding their consent or where the Trust believes disclosure will be in the best interests of the pupil or other pupils.

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

**12. SUBJECT ACCESS REQUESTS.**

Anybody who makes a request to see any personal information held about them by the Trust is making a subject access request SAR.

All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, if they constitute a "filing system." (Section 1)

All requests for a SAR should be sent to GDPR Data Protection Lead or the PA to the Headteacher / Principal. The PA To Headteacher / Principal will notify the GDPR Data Protection Lead when SAR are received.

Where a child or young person does not have sufficient understanding to make his or her own request (usually those under 12, or over 12 with special educational need which make understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The GDPR Data Protection Lead or PA To Headteacher / Principal must however be satisfied that: -

- The child or young person lacks sufficient understanding and

- The request made on behalf of the child or young person is in their interests.

Any individual including a child or young person with ownership of their own information rights, may appoint another person to request access to their records.
In such circumstances the Trust must have written evidence that the individual has authorised the person to make the application and the GDPR Data Protection Lead or PA To Headteacher must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

A subject access request must be made in writing. The Trust may ask for any further information reasonably required to locate the information.

### 12.1 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 pupil 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.

An individual only has the automatic right to access information about themselves and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.
All files must be reviewed by GDPR Data Protection Lead and Data Protection Officer before any disclosure takes place. Access will not be granted before this review has taken place.
Where the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

## 13. 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.

## 14. OTHER RIGHTS OF INDIVIDUALS.

The Trust has an obligation to comply with the rights of individuals under the law and takes these rights seriously. The following section sets how the Trust will comply with the rights to:

- Object to Processing.
- Rectification.
- Erasure.
- Data.

**Right to object to processing**.

An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest where they do not believe that those grounds are made out.

Where such an objection is made, it must be sent to the GDPR Data Protection Lead within 2 working days of receiptand in consultation with the Data Protection Officer will assess whether there are compelling legitimate grounds to continue processing which override the interest, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

The GDPR Data Protection Lead shall be responsible for notifying the individual of the outcome of their assessment within 10 working days of receipt of the objection.

**Right to rectification**.

An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to the GDPR Data Protection Lead within 2 working days of receipt and where adequate proof of inaccuracy is given, the data shall be amended as soonas reasonably practicable and the individuals notified.

Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data and communicated to the individual. The individual shall be given the option of either a review by the Data Protection Officer or an appeal direct to the Information Commissioner.

An individual also has a right to have incomplete information completed by providing the missing data and any information submitted in this way shall be updated without undue delay.

**Right to erasure**.

Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arise in the following circumstances.

- Where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed.

- Where consent is withdrawn and there is no longer other legal basis for the processing. Where an objection has been raised under the "Right to Object" and found to be legitimate. Where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met).
- Where there is a legal obligation on the Trust to delete.

The GDPR Data Protection Lead will make a decision regarding any application for erasure of personal data and willbalance the request against the exemptions provided for in the law. Where a decision is made to erase the data and this data has been passed to other data controllers and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

**Rights to restrict processing**

In the following circumstances, processing of an individual's personal data may be restricted:

- Where the accuracy of data has been contested, during the period when the Trust is attempting to verify the accuracy of the data.
- Where processing has been found to be unlawful and the individual has asked that there be a restriction on processing rather than erasure.
- Where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim.
- Where there has been an objection made under the Right to Object pending the outcome of any decision.

**Right to portability.**

If an individual wants to send their data to another organisation, they have a right to request that the Trust provides their information in a structured, commonly used and machine readable format. As this right is limited to situations where the Trust is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be quite limited. If a request for this is made, it should be forwarded to the GDPR Data Protection Lead within 2 working days of receipt and they will review and process as necessary.

## 15. 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.

## 16. BREACH OF ANY REQUIREMENT OF THE GDPR.

All breaches of the GDPR, including a breach of any of the data protection principles, shallbe 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 hoursof 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 andcategories 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 tomitigate 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 this 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.

**CONTACT**

If anyone has any concerns or questions in relation to this Policy, they should contact the GDPR Data Protection Lead or the Data Protection Officer.

## 17. Biometric recognition systems

(Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18).

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.

## 18. CCTV

We use CCTV in various locations around the Trust's school / academy sites to ensure they remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

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

**Purpose**

The purpose is to regulate the management, operation and use of the closed-circuit television system for the schools / academies within the Five 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 I.T. department are the people who have been appointed to oversee the system and procedures.

**Quality Control**

A regular maintenance program 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:

- Sixth form administration staff
- Lettings team staff
- Site team staff

Access to view live and recorded images is restricted to:

- Members of the leadership group
- Year Leaders
- Sixth Form Attendance Staff
- IT Network Manager (or other delegated person in his 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.

## 19. Photographs and videos

As part of our Trust School or Academy activities, we may take photographs and record images of individuals within our Trust.

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

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

Photography and videos at school / academy events are not permitted to be taken by parents/carers, students, staff, or visitors. Special dispensation may be given for specific events where permission will be gained in advance.

Where the Trust schools / academies take photographs and videos, uses may include:

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

## 20. Data security and storage of records

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 appendix 1.
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 pupils 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 pupils

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 personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops, and other electronic devices. Staff and pupils 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, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust-owned equipment (see our 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)

## 21. Personal data breaches

The Trust 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 below.
When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it.

### 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.
The Data Protection Officer will investigate the report and determine whether a breach has occurred.
To decide, the Data Protection Officer 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 and governors will cooperate 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 Data Protection Officer will alert the headteacher and the chair of governors.
- The Data Protection Officer will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the Data Protection Officer with this where necessary, and the Data Protection Officer should take external advice when required.
- The Data Protection Officer 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 Data Protection Officer will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool

The Data Protection Officer 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 computer system.

Where the ICO must be notified, the Data Protection Officer 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 data protection officer 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 Data Protection Officer
- 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 Data Protection Officer 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 Data Protection Officer expects to have further information. The Data Protection Officer will submit the remaining information as soon as possible

Where the school / academy is required to communicate with individuals whose personal data has been breached, the Data Protection Officer 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 Data Protection Officer
- 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 Data Protection Officer 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 Data Protection Officer 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 Data Protection Officer area of the Trust computer systems.

The Data Protection Officer, School / Academy GDPR Data Protection Leads, and Operations Manager 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 Data Protection Officer and Operations Manager will meet regularly 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.

**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 Data Protection Officer as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the Data Protection Officer will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the school's / academy'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 Data Protection Officer will consider whether it is 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 Data Protection Officer / GDPR Data Protection Leads will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The Data Protection Officer 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 Data Protection Officer will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 safeguarding partners.

**FREEDOM OF INFORMATION**.

1. **Introduction**

The Trust is subject to the Freedom of Information Act 2000 (FOI) as a public authority, and as such, must comply with any requests for information in accordance with the principles laid out in theAct.

2. **WHAT IS A REQUEST UNDER FOI**

Any request for information from the Trust is technically a request under the FOI, whether the individual making the request mention the FOI.
However, the ICO has stated that routine requests for information (such as parent requesting a copy of policy) can be dealt with outside of the provision of the Act.

In all non-routine cases, if the request is simple and the information is to be released, then the individual who received the request can release the information, but must ensure that this is done within the timescales set out below. A copy of the request and response should then be sent to the GDPR Data Protection Lead.
All other requests should be referred in the first instance to GDPR Data Protection Lead or PA To Headteacher who may allocate another individualto deal with the request. This must be done promptly and in any event within 3 working days of receiving the request.

When considering a request under FOI, you must bear in mind that release under FOI is treated as release to the general public, and so once it has been released to an individual, anyone can then access it, and you cannot restrict access when releasing by marking the information “confidential” or “restricted”.

3. **TIME LIMIT FOR COMPLIANCE**

The Trust must respond as soon as possible and, in any event, within 20 working days of the date of receipt of the request. For the Trust, when calculating the 20 working days deadline, a “working day” is a school / academy day (one in which the pupils are in attendance), subject to an absolute maximum of 60 normal working days (not school / academy days)” to respond.

4. **PROCEDURE FOR DEALING WITH A REQUEST**

When a request is received that cannot be dealt with by simply providing the information, it should be referred in the first instance to the GDPR Data Protection Lead, who may re allocate to an individual with responsibility for the type of information requested.

The first stage in responding is to determine whether the Trust “holds” the information requested. The Trust will hold the information if it exists in computer or paper format. Some requests will

require the Trust to take information from different sources and manipulate it in some way. Where this would take minimal effort, the Trust is considered to "hold" that information, but if the required manipulation would take a significant amount of time, the requestor should be contacted to explain that the information is not held in the manner requested, and offered the opportunity to refine their request. For example, if a request required the Trust to add up the totals in a spreadsheet and release the total figures, this would be information "held" by the Trust. If the Trust would have to go through a number of spreadsheets and identify.

Individual figures and a provide a total, this is likely not to be information "held" by the Trust, depending on the time involved in extracting the information.

The second stage is to decide whether the information can be released, or whether one of the exemptions set out in the Act applies to the information. Common exemptions that might apply include:

- Section 40 (1) – The request is for the applicant's personal data. This must be dealt with the subject access regime in the DPA, detailed in paragraph 9 of the DPA policy.
- Section 40 (2) – Compliance with the request would involve releasing third party data, and this would be in breach of the DPA principles as section 3 of the DP policy
- Section 41 – Information that has been sent to the Trust (but not the Trust's own information) which is confidential.
- Section 21 – Information that is already publicly available, even if payment of a fee is required to access that information.
- Section 22 – Information that the Trust intends to publish at a future date.
- Section 43 – Information that would prejudice the commercial interests of the Trust and / or a third party.
- *Section 38 – Information that could prejudice the physical health, mental health or safety of an individual (this may apply particularly to safeguarding information).*
- *Section 31 – Information which may prejudice the effective detection and prevention of crime – such as the location of CCTV cameras.*
- *Section 36 – Information which, in the opinion of the chair of governors of the School, would prejudice the effective conduct of the School. There is a special form for this on the ICO's website to assist with the obtaining of the chair's opinion.*

The sections mentioned in italics are qualified exemptions. This means that even if the exemption applies to the information, you also have to carry out a public interest weighing exercise, balancing the public interest in the information being released, as against the public interest in withholding the information.

**RESPONDING TO A REQUEST**.

When responding to a request where the Trust has withheld some or all of the information, the Trust must explain why the information has been withheld, quoting the appropriate section number and explaining how the information was requested fits with that exemption. If the public interest test has been applied, this also needs to be explained.
The letter should end by explaining to the requestor how they can complain – either by reference to an internal review by (a governor), or by writing to the ICO.

**CONTACT**

Any questions about this policy should be directed in the first instance to the GDPR Data Protection Lead or Data Protection Officer.

# 1. Appendices

## (1) Contact

The School / Academy specific GDPR Data Protection Leads are:

- The Hazeley Academy Stephen Whitney
- Shenley Brook End School Louise Moore

The PA to the Headteachers / Principals are:

- The Hazeley Academy Eloise Cooke
- Shenley Brook End School Nadine Lannin

Please contact the staff above for Freedom of Information or Subject access requests.

The DPO Data Protection Officer (DPO) for the Trust is:

- Greg Cunningham

Breaches of the Policy/Code

Any breach of this policy or the Code of Practice by school / academy staff will be formally investigated and may result in disciplinary action.