ACHIEVING TOGETHER

FOUR STONES GATEWAY TRUST

DATA PROTECTION POLICY

DATE POLICY WAS APPROVED	20.10.2025
DATE POLICY WILL BE REVIEWED	Autumn 2026
MEMBER OF STAFF WITH RESPONSIBILTY FOR REVIEW	Head of IT Services

Key Definitions

All policies incorporate the following schools or organisations within Four Stones Gateway Trust ('the Trust'):

- Clee Hill Community Academy
- Cleobury Mortimer Primary School
- Haybridge High School and Sixth Form
- Haybridge Teaching School Hub
- Haybridge SCITT
- King Charles I School
- Lacon Childe School
- SHaW (Shropshire, Herefordshire and Wolverhampton) Maths Hub
- Stottesdon CofE Primary School
- TDMS (The De Montfort School)
- Any other schools or organisations that may join the Trust from time to time and not listed above.

The terms Academy, School, Organisation and Trust are considered interchangeable in the context of all Trust policies.

Where appropriate, in this Policy the term:

"CEO" includes the Chief Executive Officer

"CFOO" includes the Chief Financial Officer

"Trust Senior Leadership Team" includes Executive Headteachers, Headteachers, strategic operational leads and Teaching School/SCITT Directors.

"Headteacher" includes the appropriate School Headteacher.

"Trustees or Trust Board" are appointed Trustees who oversee the business of Four Stones Gateway Trust, agreeing the overarching strategic direction and ensuring robust governance.

"Local Academy Boards (LAB)" are appointed Governors at a local level associated with the Trust's Worcestershire Schools. LAB Governors act as advocates for their school's Safeguarding, SEND, Standards and Stakeholder engagement.

"Local Governing Bodies (LGB)" are appointed Governors at a local level associated with the Trust's Shropshire Schools. LGB Governors are advocates for their school's Safeguarding, SEND, Standards and Stakeholder engagement.

"Chair" responsible for leading the board and ensuring its effectiveness

"Stakeholders" are any individuals or companies who are invested in the welfare and success of the Trust and/or School and its students, including staff members, students, parents, community members, LAB, LGB or Trust members, trade unions, local business leaders etc.

Contents

1. Aims 3
2. Legislation and guidance 3
3. Definitions....3
4. The data controller....4
5. Roles and responsibilities 4
6. Data protection principles 5
7. Collecting personal data 5
8. Sharing personal data....6
9. Subject access requests and other rights of individuals 7
10. Parental requests to see the educational record 8
11. Biometric recognition systems 8
12. CCTV....9
13. Photographs and videos 9
14. Data protection by design and default....10
15. Data security and storage of records 10
16. Disposal of records....11
17. Personal data breaches....11
18. Training 11
19. Monitoring arrangements....11
20. Links with other policies....11
Appendix A: Contact Information Data protection officer (DPO)/representative (DPR)....13
Appendix B: School Records Management....14
Appendix C: Subject access request form 15
Appendix D: Personal data breach procedure 17

1. Aims

The Four Stones Gateway Trust (the Trust) aims to ensure that all personal data collected about Staff, Students, Parent/Carers, Members, Trustees, Governors, Visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UKGDPR) and the provisions of the Data Protection Act 2018 (DPA 2018). This Policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

- This Policy meets the requirements of the UKGDPR and the expected provisions of the DPA 2018.
- It is based on guidance published by the Information Commissioner's Office (ICO) on the UKGDPR and the ICO's code of practice for subject access requests.
- It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.
- It reflects the ICO's code of practice for the use of surveillance cameras and personal information.
- 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.
- 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, individual. This may include the individual's: ▪ Name (including initials) ▪ Identification number ▪ Location data ▪ Online identifier, such as a username ▪ Image (including photo and video) 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/carers, students, staff, members, Trustees, Governors, visitors, and others, and therefore is a data controller. The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required. The Trust ICO registration number is ZA521971.

5. Roles and Responsibilities
This Policy applies to **all staff** employed by the 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 Trust Board
The Trust Board has overall responsibility for ensuring that our schools comply with all relevant data protection obligations.

5.2 Data Protection Officer (DPO)
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 Trust Board and, where relevant, report to the Board their advice and recommendations on school data protection issues. The DPO is the first point of contact for the ICO. Full details of the DPO's responsibilities are set out in their job description.

Please see Appendix A for the relevant contact details.

5.3 Data Protection Representative (DPR)
Each school in the Trust has a Data Protection Representative (DPR). The role of the DPR is to support the Trust's DPO, oversee the implementation of this Policy and other related policies in their school, monitor their school's compliance with data protection law and provide staff training in line with the DPO's guidance. The DPR is also the first point of contact for individuals whose data the school processes. Full details of the DPR's responsibilities are set out in their job description. Please see Appendix A for the relevant contact details.

5.4 CEO
The CEO is responsible for ensuring that the Data Protection Policy and guidelines are being adhered to.

5.5 Headteachers
The Headteacher of the individual school's act as the data controllers on a day-to-day basis.

5.6 Information Asset Owners
The Trust has also identified Information Asset Owners (IAOs) for the various types of data being held in each school (e.g., student/ staff information, assessment data etc.). These IAOs will manage and address risks to the information and understand what information is held and for what purpose, how information has been amended or added to over time, and who has access to protected data and why. They will ensure that information in their care is protected by an appropriate level of security, though, for example, password protection or where necessary, encryption. Please see Appendix B for the current appointees.

5.7 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
- Only using personal data for purposes that are authorised by the Trust.
- Using Trust approved systems and devices to process personal data.
- Storing and transferring personal data in a secure manner, using systems approved by the Trust.
- Contacting the DPR in the following circumstances:
  - If there has been a data breach
  - If they receive a request from an individual who wishes to access records containing personal data
  - 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 they intend to use online resources, or AI technologies that require the personal data of students or staff
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need to share personal data with third parties who provide services, online resources, or support to their school

5.8 Parents/carers
All parents/carers are responsible for:
- checking that any information they provide to the relevant school within the Trust is accurate and up to date.
- informing the relevant school within the Trust of any changes to information which they have provided, e.g., changes of address, telephone numbers.
- informing the relevant school within the Trust of any errors in the information that the school holds about them.

The Trust cannot be held responsible for any errors of which it has not been informed.

6. Data protection principles
The UKGDPR is based on data protection principles that the Trust 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 Trust aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness, and transparency
We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

- The data needs to be processed so that the individual schools within the Trust can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering a contract.
- The data needs to be processed so that the individual schools within the Trust can **comply with a legal obligation.**
- The data needs to be processed to ensure the **vital interests** of the individual e.g., to protect someone's life.
- The data needs to be processed so that the schools within the Trust, as a public authority, can perform a task **in the public interest,** and carry out its official functions.
- The data needs to be processed for the **legitimate interests** of the individual schools within the Trust 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 one of the special category conditions for processing which are set out in the UKGDPR and Data Protection Act 2018.

If we offer online services to students and we intend to rely on consent as a basis for processing, we will get parental consent where the student is under 13 (except for online counselling and preventive services).

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

7.2 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 to do their jobs.

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 our Records Management and Retention Policy. See Appendix B for further information on records retention and management.

8. Sharing Personal Data
We will not normally share personal data with anyone else, but may do so where:
- We have informed you about sharing arrangements in a Privacy Notice
- 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 which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, 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, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:
- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

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

Where we transfer personal data to a country or territory outside the UK, we will do so in accordance with data protection law.

9. Subject Access Requests and other Rights of Individuals

9.1 Subject Access Requests (SARs)

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust 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, shared with
- How long the data will be stored for, or if this is not possible, the criteria used to determine this period.
- 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.

If staff receive a subject access request, they must immediately forward it to the relevant DPR.
Please see Appendix C for further information on how to make a subject access request.

9.2 Children and Subject Access Requests (SARs)

Personal data about a child belongs to that child, and not the child's parents/carers. For a parent/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 aged 13 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/carers of students at our individual schools 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.

Where a parent/carer makes a subject access request on behalf of a student who is over the age of 13, the relevant staff from school will consult with the DPO to determine whether the request can be processed without consent (where the request is in the interest of the child).

9.3 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.
- 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 will not disclose records if they:

- Contain the personal data of other individuals and redaction of the record is not possible.
- Might cause serious harm to the physical or mental health of the student or another individual.
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information. When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO.

Please see Appendix C for further information on how to make a subject access request.

9.4 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, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest.
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, which might negatively affect them)
- Prevent processing that is likely to cause damage or distress.
- 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 relevant DPR. If staff receive such a request, they must immediately forward it to the relevant DPR.

10. Parental Requests to see the Educational Record
Under data protection legislation, parents/carers and students have the right to request access to information about them that we hold.

To make a request for your personal information, or be given access to your child's educational record, please contact the school.

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress.
- Prevent it being used to send direct marketing.
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted, or destroyed, or restrict processing.
- Claim compensation for damages caused by a breach of the data protection regulations.

To exercise any of these rights, please contact the relevant DPR (see Appendix A).

11. 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 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 individual schools 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 school's biometric system(s). We will provide alternative means of accessing the relevant services for those students. For example, students can pay for school dinners using a pin number instead.

Parents/carers and students can object to participation in the school's biometric recognition system(s), or 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 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.

12. CCTV

We use CCTV in various locations around our school sites to ensure the security of our school environments, help us undertake our safeguarding duties in relation to staff and students, and to assist us in managing behaviour in school. The Trust has a CCTV Policy which governs the use of CCTV systems in operation at our schools.

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.

The CCTV systems in use across the Trust do not support the redaction of live footage. Where an information request relates to CCTV footage, this may be fulfilled through the disclosure of redacted still images.

13. Photographs and Videos

As part of our individual schools' activities, we may take photographs and record images of individuals within our schools. We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students, where these are intended for external use (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 student. Where we do not need parental consent, we will clearly explain to the student how the photograph and/or video will be used. Uses may include:

- For the profile picture on the school's information management system
- For examination submissions
- Performing arts including dance and movement, concerts, and drama performances
- Sports days and sports fixtures and the use of photographic equipment by parents/carers
- Media, including newspapers and television
- Displays in school.
- The school's website-e.g. prospectus and other publications.
- The school's social media accounts
- Staff training and professional development activities
- Site security CCTV videos

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.

To withdraw or amend consent preferences, please contact the relevant school.

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.

See our 'Photographic Images of Children' Policy for more information on our use of photographs and videos.

14. 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 privacy impact assessments where the Trust's or its constituent 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
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our schools, DPO and DPRs 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

15. 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:

- All staff are responsible for ensuring that any personal information, which they hold, or for which they are responsible, is kept securely. This could include information about a variety of members of the school community- including students, staff, and parents/carers- e.g., legal guardianship issues, disciplinary records, progress records, reports, references, employment history, taxation and national insurance records, or appraisal records. Staff are also responsible for taking particular care when handling "sensitive personal data"- for a student this would include if they had special educational needs or if they were a "looked after child," medical information relating to them, child protection issues relating to them, their religious beliefs, or political opinions, their physical or mental health issues or their sexual orientation. This would also include more logistical items such as addresses, phone numbers or dates of birth.
- Records containing personal information must be stored in appropriate Trust systems.
- Records containing personal information must not be downloaded to or transferred to personal devices.
- Personal information stored in electronic documents must be password protected.
- Computers, laptops, tablets, mobile phones and other personal devices used to store or access personal information must be locked whenever they are left unattended.
- Personal information must be kept on the network storage facilities provided.
- Personal information that is collected or processed over the internet must only be accessed via a secure encrypted connection using username authentication to prevent unauthorised disclosure.
- Personal information must not be transferred via email.
- Personal information must not be disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops, and other electronic devices. Staff and students are reminded to change their passwords at regular intervals.
- The use of portable storage devices and removable media, such as USB memory keys and portable hard drive is not permitted.
- Staff, students, Members, Trustees, 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 IT Acceptable Use & Online Safety 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)
- All staff must abide by the rules laid out in the Trust's 'IT Acceptable Use & Online Safety' Policy, including the 'Data Protection in the classroom' section.

See Appendix D for further information on records retention and management.

16. Disposal of Records

The Trust maintains a retention schedule which informs the safe destruction of personal data when it is no longer required. Records may also be deleted where the DPO has approved a request for erasure made by a data subject. The disposal of data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated, or otherwise disintegrated for data. Paper files containing sensitive information should be placed in white "confidential waste" bags/Shred It bins for shredding.

17. 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 in Appendix D. When appropriate, we will report the data breach to the ICO within 72 hours.

We will take actions to mitigate the impact of different types of data breach, 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. For example: if sensitive information has been disclosed via email (including safeguarding records), we will take the following actions:

- 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 DPR as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPR will ask the IT Technical Support Department to recall it.
- In any cases where the recall is unsuccessful, the DPR will 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 DPR will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPR 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.

Other breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on one of our school's websites 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
- A school's cashless payment provider being hacked, and parents' financial details stolen.

18. Training

All staff, Trustees, and Governors are provided with data protection training as part of their induction process.

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

19. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this Policy. It will be reviewed annually and shared with the Trust Board.

20. Links with Other Policies

This Data Protection Policy is linked to our:

- Freedom of information publication scheme
- Privacy Notices for: staff, students, parents/carers, job applicants, Haybridge SCITT trainees, Members, Trustees, and Governors
- Photographic Images of Children Policy
- Online Safety and IT Acceptable Use Policy
- Safeguarding Policy (including Child Protection)

Appendix A: Contact Information Data protection officer (DPO)/representative (DPR)

Contact	Phone	
James Plant - DPO	01562 826580	DPO@fourstonesgateway.org.uk
Julia Priscott - DPR Clee Hill Community Academy	01584 890384	admin@chcacademy.co.uk
Julia Priscott - DPR Cleobury Mortimer Primary School	01299 270313	head@cmpschool.co.uk
Julia Priscott - DPR Haybridge High School	01562 886213	office@haybridge.worcs.sch.uk
James Wilkinson - DPR King Charles I School	01562 512880	office@kingcharles1.worcs.sch.uk
Julia Priscott - DPR Lacon Childe School	01299 270312	admin@laconchildeschool.co.uk
Julia Priscott - DPR Stottesdon CofE Primary School	01746 718617	admin@stottesdon-school.co.uk
Jenni Dunn - DPR The De Montfort School	01386 442060	office@tdms.worcs.sch.uk

Appendix B: School Records Management

The Trust recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the school and provide evidence for demonstrating performance and accountability. This appendix provides the Policy framework through which this effective management can be achieved and audited. It covers:

- Scope
- Responsibilities
- Relationships with existing policies
- Retention times

1. Scope

1.1 This appendix applies to all records created, received, or maintained by staff of the school in the course of carrying out its functions.

1.2 Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received, or maintained in hard copy or electronically.

1.3 A small percentage of the school's records might be selected for permanent preservation as part of the institution's archives and for historical research.

2. Responsibilities

2.1 The Trust has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this is the CEO/Executive Headteacher.

2.2 The person responsible for records management in the school will give guidance for good records management practice and will promote compliance with this Policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this appendix by surveying at least annually to check if records are stored securely and can be accessed appropriately.

2.3 Individual staff and employees must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with the Trust's records management guidelines.

3. Retention Guidelines

The Trust follows the retention guidelines issued by the Management Society of Great Britain 'Retention Guidelines for Schools'. Some retention periods are governed by statute and others are guidelines following best practice. Every effort has been made to ensure that these retention periods are compliant with the requirements of the General Data Protection Regulation (UKGDPR) and the Freedom of Information Act 2000. Managing record series using these retention guidelines will be deemed to be 'normal processing' under the legislation mentioned above. If records are to be kept for longer or shorter periods than laid out in this document, the reasons for this will be documented.

Additional reference material:

Record Keeping and Retention information for Academies (Department of Education)

Appendix C: Subject Access Request Form

The General Data Protection Regulation (UKGDPR) provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Students who are 13 or above must make a Subject Access Request themselves.

If you wish to see your information, you can request this by contacting the relevant data protection officer (please see Appendix A) or by completing the form below. You will also be required to provide proof of your identity before we can process the SAR. Your request will be processed within 30 calendar days upon receipt of a fully completed form and proof of identity.

Proof of Identity
For Parents/carers who make requests on behalf of students, we require proof of your identity before we can disclose any personal information. We require you to provide two documents as proof of your identity, one should include a photograph and should include your name, date of birth and/or current address. If you have changed your name, please supply relevant documents evidencing the change. The following documents are acceptable:

- birth certificate
- passport
- driving licence
- official letter addressed to you at your address e.g. bank statement, recent utilities bill or council tax bill.

Administration Fee
There is no charge for Subject Access Requests. However, there may be a charge for providing duplicate information and/or dealing with excessive requests. The charge will be based upon the amount of time spent dealing with the request.

Please complete the following sections of this form providing as much information as possible to help us deal with your request.

Section 1
Provide details of the person(s) about whom the Trust is holding data (the Data Subject)

Full name (Print)			
Date of Birth			
Present address		**Previous address**	
Post code		**Post code**	
Telephone number			
Email address			

Section 2
Are you requesting information about yourself (person referred to in Section 1)? If **YES**, please continue to Section 3. If **NO**, please complete the following:

Full name (Print)	
Present address	

Post code	
Telephone number	
Email address	
Relationship with data subject & brief explanation as to why you are requesting this information rather than the data subject	

If you are acting on behalf of the data subject you will need to enclose their written authority including a signature or other legal documentation (e.g. power of attorney) to confirm this request. You also need to enclose evidence of your identity and that of the data subject (see Section 4 for details of acceptable identity)

Section 3
Please provide a clear description of the information that you are requesting, see table below.

If you provide specific details of what information you want, e.g. name of a document relevant to a time period rather than just the whole of your file you may receive a quicker response.

Description of Information	Trust Staff Member Holding this Information	Time Period for Information Requested

Section 4
Please provide two pieces of evidence of your identity (one containing a photo). Acceptable types of documents used to verify your identity are detailed below.

Driving Licence	Passport	National ID Card	Medical Card	Utility Bill

Section 5
All information in respect to your request will be sent to you via secure email unless you make alternative arrangements with the school/Trust. We may require further evidence of your identity if you collect your information from school premises.

Declaration

To be completed by all applicants. Please note that any attempt to mislead the school/Trust may lead to prosecution.

I (insert name) _____ certify that the information given on this application form and any attachments therein is accurate and true.

I understand that it is necessary for the school/Trust to confirm my identity and it may be necessary to obtain more information in order to locate the correct information.

Signature	
Date	

Appendix D: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

1. **Reporting a Breach**

   If a staff member or data processor finds or causes a breach (or potential breach), they must **immediately notify the relevant Data Protection Representative (DPR)**.
   The DPR alerts the **Data Protection Officer (DPO)** and seeks advice regarding investigation.

2. **Investigation by DPR**

   The DPR investigates the report and decides whether a breach has occurred.
   A breach may involve personal data being:
   - Lost
   - Stolen
   - Destroyed
   - Altered
   - Disclosed or made available where it should not have been
   - Made available to unauthorised people

   The DPR discusses findings with the DPO.

3. **Containment and Impact Assessment**

   The DPR leads efforts to **contain the breach and minimise its impact**, with support from staff or data processors as needed.
   The DPR assesses potential consequences based on severity and likelihood and provides a written report to the DPO.

4. **Escalation and Notification**

   The DPO alerts:
   - The relevant Headteacher
   - The CEO (who will notify the Chair of the Trust Board)

   The DPO decides whether the breach must be reported to the **Information Commissioner's Office (ICO)**, based on whether it poses risks to individuals' rights and freedoms (e.g. identity theft, financial loss, discrimination, emotional distress, reputational harm).

5. **ICO Notification (if required)**

   If ICO notification is required, the DPO must report via the ICO "report a breach" page within **72 hours**.
   Report must include (where possible):
   - Categories and approximate number of individuals affected
   - Categories and approximate number of records affected
   - Contact details of the DPO
   - Description of the consequences
   - Description of measures taken/being taken

   If all details are not available within 72 hours, the DPO submits what is known, explains the delay, and provides missing details as soon as possible.

6. **Informing Affected Individuals**

   The DPO assesses whether there is a **high risk** to individuals.
   If yes, the DPO must promptly inform affected individuals in writing, providing:
   - DPO contact details
   - Likely consequences of the breach
   - Measures taken to mitigate impact
   - The DPO also informs relevant third parties who can help (e.g., police, banks, insurers).

7. Record-Keeping

The DPO documents every breach, whether reported to the ICO or not.
Each record must include:

- Facts and cause
- Effects
- Actions taken to contain and prevent recurrence

Records are stored securely on the school system.

8. Review

The DPO, DPR, and relevant Headteacher/CEO meet to review the breach and agree measures to prevent recurrence.

This review is held **as soon as reasonably possible** after containment.