DATA PROTECTION POLICY

For

Stretford Grammar School

June 2023

Contents

Data Protection Policy

1. Introduction

Stretford Grammar School must process personal information to fulfil its services as an education provider. When processing personal information, the school has an obligation to ensure it not only remains secure and protected but also meets the high standards of data protection compliance set by the UK government.

The school currently process the personal data of the following individuals:

- Students
- Parents & Carers
- Staff (including temporary and voluntary staff)
- Governors
- Visitors to School
- Third Parties such as Contractors and Consultants that provide services to School.

This policy outlines how the school comply with data protection legislation and the steps taken to maintain the security, integrity and confidentiality of personal information.

This policy applies to all personal data processed by the school in both physical and electronic records. It also applies to third party organisations that process data on our behalf (Data Processors).

Appendix A provides a breakdown of useful terms referenced in this policy.

2. Legislation & Guidance

When processing personal data, the school must meet the provisions set out in the following legislation:

- UK General Data Protection Regulation (UK-GDPR) 2021
- Data Protection Ace (DPA) 2018
- Education (Pupil Information) (England) Regulations 2005
- Protection of Freedoms Act (2012) – Use of Pupil Biometric Data

The school follow guidance from the following parties when processing personal data:

- Information Commissioners Office (ICO)
- Department for Education (DfE)
- Information & Records Management Society (IRMS – Toolkit for Schools)

3. The data controller

Stretford Grammar School is the Data Controller for the personal information that we process, this means that we are responsible for that data and make decisions on how it is processed. The school is registered as a Data Controller with the ICO and pays an annual renewal fee.

The DfE act as a Joint Data Controller for certain data that the school must submit to them to meet our legal obligations as a school.

4. Roles and responsibilities

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

Governing Board

The governing board has overall responsibility for ensuring that the school complies with all relevant data protection obligations.

Headteacher

The headteacher acts as a representative of the school as Data Controller on a day-to-day basis and ensures adequate resources are allocated to allow effective implementation of this policy.

Data Protection Officer

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

The DPO will provide an annual report of their activities directly to the governing 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 and Data Subjects. The DPO of Stretford Grammar School is Mr Owen Chadbond supported by Miss Danielle Eadie of RADCaT Ltd who the school has nominated to support and advise on more technical data protection matters. The DPO team can be contacted using the following details: T: 0161 865 2293 | E: dpo@stretfordgrammar.com.

School Staff

The school ask that all staff comply with the provisions set out in this policy when processing personal data. Breaches of this policy may result in disciplinary action.

The DPO should be contacted by staff in the following scenarios:

- 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 process 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 United Kingdom.
- If there has been a data breach (or near miss).
- 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. Data protection principles

The UK-GDPR sets out six key principles that the school must comply with to ensure personal data is:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes (purpose limitation).
- Adequate, relevant, and limited to what is necessary to fulfil the purposes for which it is processed (data minimisation).

- Accurate and, where necessary, kept up to date (data accuracy).
- Kept for no longer than is necessary for the purposes for which it is processed (storage limitation).
- Processed in a way that ensures it is appropriately secure.

The school must also demonstrate how it complies with the principles above to meet the UKGDPR's overarching principle 'accountability'.

The following sub sections outline how the school comply with these principles:

6. Lawfulness, fairness and transparency

Lawfulness

To process personal data lawfully, the school meet one of the following lawful bases (legal reasons) from Article 6 of the UK-GDPR:

- The individual has provided clear consent for the school to process their data for instance when seeking permission to use images on the school website.
- The processing of the data is necessary to fulfil a contract with the individual such as the terms of an employment contract.
- Personal data is being processed to meet a legal obligation for example when keeping a record of who is on site to meet fire safety requirements under health & safety law.
- The processing is necessary to perform a task in the public interest or part of our official functions of a school. This typically applies when processing data to meet our statutory obligations as an education provider.
- 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 for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)

For special categories of personal data (information that is more sensitive in nature), the school meet an additional lawful basis from Article 9 of the UK-GDPR:

- Explicit consent has been provided by the individual.
- Processing is necessary for reasons of employment, social security, and social protection.
- Special category personal data needs to be processed in order to protect or save someone's life; ensure their vital interests.
- Processing is necessary for the legitimate activities of a not-for-profit body.
- The personal information has been made public by the individual.
- Processing is necessary for legal claims and judicial acts.
- Processing is necessary for reasons of substantial public interest.
- Processing is necessary for health or social care.
- Processing is necessary for reasons of public interest in the area of public health.
- Processing is necessary for archiving, research and statistics in the public interest.

Consent & Parental Consent

Where consent is the lawful bases for processing, individuals are provided with a clear and written consent form that includes what data is processed, how and why it is processed and instructions on how to withdraw consent or change their preferences; a log of consent is kept on the school's information management system and updated where necessary.

Under data protection law, a childs personal data belongs to that child and not their parent or carer. The school however understand that dependent upon age, a child may not be mature enough to understand data protection and their rights.

As a rule of thumb, the school will obtain any consent required from the parents or carers of children in years 7 and 8 whilst those in years 9 and above will provide consent themselves. Considerations are however taken for vulnerable students that may not have the ability to understand their rights regarding data protection.

Fairness & Transparency

The school provide clear information to all individuals about the processing of their data via the use of 'Privacy Notices'. At the point of any data capture, individuals will be informed on whether processing is mandatory or optional.

7. Purpose limitation

The school only collect personal data for specified explicit and legitimate reasons; those reasons are explained 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 are fully instructed on what data they are permitted to process as part of their role and are asked to seek permission if they are asked to process information for a new purpose.

8. Data Minimisation

The school adopt a minimalist approach to data processing and only collect the categories of information necessary to fulfil the purposes for which it is collected. Key information management systems used by the school are designed to ensure data capture fields are limited to what is necessary.

The school carefully review the pupil admission and staff induction processes to ensure that only the data required to meet our legal, statutory, and operational duties are collected.

Our minimalist approach also applies to data sharing; if we must transfer data to a third party, a review will take place to ascertain the minimum amount of data necessary to meet the purpose of collection.

9. Data Accuracy

Personal data for staff and students is reviewed on a routine basis as part of the school census process; the school has a statutory obligation to submit up to date and accurate information about staff and students to the DfE.

Parents are prompted on routine intervals to inform the school if there has been a change in details or circumstances that the school need to be aware of. For students with special educational needs or where there are safeguarding concerns, regular communication is made with the relevant parties to ensure that information is up to date and accessible to the right person(s) to provide adequate support.

The school have implemented key systems and processes that help to ensure personal data is updated on a routine basis. Pupil attendance for instance is updated twice daily on the schools information management system and visitors input up to date details each time they visit.

10. Storage Limitation (Retention & Disposal of Records)

The school has statutory obligations to retain certain records for set periods of time. Industrybased guidance and school procedure are also used to determine non-statutory retention periods. Our retention schedule is set out in the school 'Records Management Policy'.

Regular reviews of records are made on a departmental level at least once a year to ensure any data no longer required is securely disposed of. Staff are asked to organise records in chronological order of deletion to support effective records management. Records that are incomplete or inaccurate will also be disposed of securely.

Physical records are disposed of via shredding whilst electronic records will be securely wiped. The school is required to keep pupil and staff records for several years once they have left the school, these records will be archived by the school until the end of their respective retention period.

The retention processes of 'Data Processors' used by the school are reviewed and logged as part of initial compliance checks and data sharing agreements to ensure they meet the standards set by the school.

Automatic deletion and anonymisation will be applied to records where applicable. The school keep an up-to-date trail of records that have been deleted.

11. Integrity and Confidentiality (Data Security)

Security of personal data plays a crucial role in the schools data protection strategy. The school ensures control measures are in place to protect both physical and electronic from unauthorised loss or disclosure. Measure include but are not limited to the following:

- A clear desk policy is in place and staff provided with lockable areas to ensure physical documents and electronic devices are locked away when not in use.

- Computer screens are positioned so they are not visible to the public; auto lock has been activated on all school owned PC's and devices. Staff are prompted to lock their screen if they leave the room or their desks.

- Areas containing records and offices are locked with key access strictly limited.

- A full permissions and access procedure is in place to ensure staff can only access the records necessary to fulfil their role. Staff sign confidentiality agreements and receive regular training on data protection and cyber security.

- Staff are provided with a user account and password to access school systems with two factor authentication used where available. Passwords are updated regularly, and staff agree not to share account details.

- A process is in place to remove staff access if they leave their employment with the school or no longer require access for their role. Access is removed on their last day of employment.

- Encryption is in place on school systems.

- Third parties with whom personal data is shared are compliance checked to ensure they make the schools high standards of security and data protection compliance. Data is shared by secure methods only.

- Data Protection Impact Assessments (DPIA) are conducted on any systems that may pose a high risk to the rights and freedoms of individuals whose data we process.

The school performs walkaround checks of the school site at intervals to identify any gaps in the security of personal data. Similarly, monitoring and reviews of key systems and processes are in place.

A data breach procedure is in place along with business continuity plans should a significant breach of security occur. The school has also implemented the following policies to support data security:

- Online Safety Policy
- Acceptable Use Policy

12. Accountability

The school understand that to comply with data protection legislation, it must be able to collectively evidence compliance. This is done by:

- clearly documenting compliance in the form of policies and procedures; all of which will be communicated to the relevant person(s)
- reviewing policies and procedures on a regular basis
- keeping logs of staff training
- keeping and updating logs of consent-based activities - keeping logs of requests related to data subject rights. - completing DPIA's where necessary
- implementing agreements with third party controllers and processors
- evidencing and monitoring any data breaches, subsequent actions and decisions made

13. Sharing personal data

Personal data is only shared with third parties where the law or school policies permit us to do so. The school will typically share personal information for the following purposes:

- Sharing data to outside agencies to provide support and ensure the safety of students, staff and other members of the school community.

- Data may be required to ensure providers of services to the school can fulfil that service, providing staff data to the payroll provider for instance.
- Sharing data with the Local Authority and DfE to meet statutory obligations.

Less commonly, personal data may be shared with:

- the emergency services if an incident occurs or for the detection / prevention of crime.
- social services if there are safeguarding concerns.
- the courts, solicitors and insurers if legal proceedings are apparent.

The school ensure that third parties are compliance checked prior to any data processing taking place by one of, or a combination of the following methods:

- Implementing data sharing agreements outlining the expectations and responsibilities of each party.
- Completing DPIA's on any high-risk data sharing activities
- Completion of a technical security questionnaire
- Keeping a copy of relevant privacy notices
- Keeping a log of the compliance process

If a situation arises where data must be transferred outside of the United Kingdom, the school ensure that appropriate safeguards are in place and the third party complies to equivalent high standards set by the school and UK government.

14. Rights of Data Subjects

Stretford Grammar School must have provisions in place to support and meet the rights that all individuals have under the UK-GDPR. The following rights are available to individuals in certain circumstances:

- The right to be informed.
- The right of access
- The right to rectification
- The right to erasure (right to be forgotten) - The right to restrict processing.
- The right to data portability
- The right to object to processing.
- Rights in relation to automated decision making and profiling.

The right to be informed:

All individuals have a right to be informed about how and why the school processes their personal information. The school meet this right by issuing 'Privacy Notices' to all individuals that includes:

- The name and contact details of the school as Data Controller - The name and contact details of the DPO.
- The categories of personal data being processed about them.
- How the information was obtained and whether processing is optional or compulsory.
- The purposes for processing their personal data.
- The lawful bases for processing (including special categories of personal data).

- The recipients of personal data if shared with third parties.
- Details if personal data is shared outside of the United Kingdom.
- Retention periods for the personal data.
- The rights available to the individual.
- The right to withdraw consent where applicable.
- The right to complain to the Trust and ICO (including instructions).

Privacy Notices are located in areas that are easily accessible to the individuals concerned.

The right of access:

All individuals have a right to ask the school about the personal data processed about them and obtain copies of that information by making a 'subject access request'.

A full procedure is in place to efficiently handle requests that is summarised as follows:

The school ask that all requests for personal information are made in writing to the DPO. The DPO will review the request and provide a proof of receipt to the individual, usually by email. At this point the school reserve the right to:

- Verify the identity of the individual if there is any doubt; proof of identity may be sought.
- Seek proof of parental responsibility if the request concerns pupil information and the requester is not listed as an authorised parent on the school register.
- Request the consent of a pupil to provide their information to their parent or carer; as a rule of thumb, consent will be required from students in year 9 and above to provide their information to their parent.
- Ask the requester to be more specific about what information they are looking to access if the request is general in nature.

A response is sent to the individual within one calendar month outlining one of the following outcomes:

1. The request has been met in full and the requested information included.
2. The school is exercising their right to extend the response time by two further calendar months as the request has been deemed complex.
3. The request has been denied, including the reasons why and relevant exemption from the Data Protection Act.

Once met in full, requests will be sent electronically in an encrypted format unless stated otherwise. All fulfilled requests will include a cover letter clearly stating what has been included and any items the school is unable to provide along with the reasons why; a copy of or directions to access the relevant privacy notice will also be included.

All staff are asked to forward any requests relating to personal information to the DPO without undue delay.

The right to rectification:

The school make reasonable attempts to ensure that personal data is complete and accurate. Any requests to rectify personal information will be reviewed accordingly. In most instances, general data such as changes in names and contact details will be rectified straight away and a confirmation provided. If an individual requests that more complex information such as meeting notes, witness statements and records relating to health and wellbeing are rectified, a full review will be conducted.

A response will be provided to the individual outlining one of the following options:

1. The review concluded that the information is indeed incorrect or incomplete and will be rectified accordingly.
2. The school disagree that the information is incorrect and refuses the request; details of the reasoning will be included along with the right to complain to the ICO should be provided with any response.

Responses and any amendments to records will be made within one calendar month.

The right to erasure:

The right to be forgotten only applies in certain circumstances; the school has legal obligations to retain personal information for set periods outlined in its 'Records Management & Retention Policy'. The right to erasure will typically apply when:

- consent is the lawful basis for processing; the processing of personal data is optional.
- the data is no longer necessary for the purpose in which it was collected.
- the processing is determined to be unlawful.
- there is a legal obligation to remove the data.

In the event that a request to be forgotten cannot be met, the individual will be provided with an explanation which includes the set retention period for their personal information.

The right to restrict processing of personal data:

Individuals have the right to ask the school to restrict the processing of their personal data if they have concerns or challenge how and why it is being processed. The school will typically restrict processing temporarily if the lawful basis for processing is challenged or if someone objects to processing whilst a review is conducted by the DPO.

In most cases, the school will be unable to meet a restriction request permanently unless the processing of personal data is optional. The DPO will provide a full explanation to the individual as to why their personal data is being processed, the applicable lawful bases and details of their right to complain to the ICO.

Right to object:

Most of the personal data processed by the school is mandatory and therefore the right to object will only apply in certain circumstances for instance where consent is the lawful basis for processing. Where processing is optional such as the use of pupil and staff images to promote the school, no further personal data will be processed and a reasonable attempt made to securely dispose of any data already processed. The school retain an active log of consent-based activities that is updated when an individual changes their preferences.

Less commonly, individuals can object to the processing of their personal data for tasks carried out in the interests of the public and on the grounds of legitimate interests. The DPO will review each of these requests accordingly. If a request is refused, compelling grounds must be demonstrated to override the rights of the individual.

Right to data portability and automated decision making:

The school does not currently partake in any data processing activities that involve automated decision making. The right to data portability is only expected to be applicable in very rare circumstances; the DPO will review any requests relating to these rights accordingly.

Responding to Data Subject Rights

All rights in respect of Data Subjects will be responded to within one calendar month and will advise the individual of their right to complain to the ICO. The school will apply a two-calendar month extension should the nature of the request be deemed complex; the individual will be informed within one calendar month of any intention to extend the likely response time.

15. Parental requests to see the educational record.

The Education Regulations (Pupil Information – England) (2005) allow parents to access their own childs educational record. This is referred to as a 'parental access request' and applies until the pupil turns 18.

A parental access request is different to a 'subject access request' under the UK-GDPR as it concerns pupil educational records only. Requests also have a shorter response time of 15 school days. It is important to note that any exemptions that would apply to a UK-GDPR request will still be applicable to a parental access request. This will typically include redacting / omitting third party data where necessary, we therefore ask that staff forward any requests for pupil information to the DPO.

Parental access requests must be made in writing and the school reserves the right to verify the identity of the individual making their request. Proof of parental responsibility will also be sought where necessary.

Pupil educational records are stored on secure information management systems that allow the school to extract specific reports for each pupil; this supports the short turnaround time for parental requests under this legislation.

The school will take the same approach to responding as it would with a UK-GDPR request and ensure parents are clearly informed if any information cannot be provided and the reasons why.

16. CCTV

The school uses 'Closed Circuit Television' (CCTV) in various locations around the school site to ensure the security of the school, safety of our staff, students, and visitors and to aid the prevention and detection of crime.

The school follows the ICO's code of practice for the use of CCTV and has implemented a CCTV Policy that is available on the school website.

The school does not need to ask individuals' permission to use CCTV but must make it clear when individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

A DPIA is completed prior to the installation or amendment of any CCTV system used in the school to assess the potential risks to the rights and freedoms of individuals.

The CCTV Policy provides information on requests to access footage captured on CCTV. The policy also outlines information on retention of images and security measures in place.

17. Biometric Data

The school use 'Biometric Data' to manage pupil and staff access to certain services in school; this includes the scanning of pupil fingerprints to access the school lunchtime ordering and payment system.

When processing biometric data of children under the age of 18years old, the school must comply with the 'Protection of Freedoms Act' which requires us to obtain parental consent prior to processing such information.

The school has implemented a 'Biometric Data Policy' that outlines the school's approach to maintaining compliance with both data protection law and the Protection of Freedoms Act.

The school conduct a DPIA on all biometric data systems prior to the processing of any biometric data. Alternative provisions are in place for any students and families that choose not to consent to this type of data processing.

18. Images

From time to time the school uses images of our students and staff to promote the school, celebrate achievements and give the wider community an insight into school life. Images refer to photographs and videos.

Students and parents are provided with a consent form that clearly informs them how and why the school uses images. The form also includes instructions on how to withdraw consent or change their preferences. An active log of pupil consent (and non-consent) is kept on the schools information management system.

The use of pupil images is typically limited to internal displays, the school website, newsletters, online educational platforms, our social media channels, and the school photographer. The school will gain specific consent from students and parents if on occasion, we are asked for students to appear in more widespread media such as the newspaper or television.

The school seek written consent from staff for the use of their images where necessary on an ad-hoc basis. All individuals are reminded of their right to withdraw consent prior to any images being taken.

If at any time consent is withdrawn, the school will perform a reasonable search to ensure any images held are securely destroyed. No further processing of images will take place and in the case of students, their consent status will be updated on their pupil profile.

Images are not accompanied by names or any other identifying information unless consent is in place to do so. The use of pupil images has been implemented into the school safeguarding policy.

19. Data Protection by Design & Default

The school understand that for data protection to be implemented effectively, the key principles of the UK-GDPR must form an integral part of the school's culture. Measures include:

- Appointing a suitably qualified DPO and ensuring they have adequate resources to fulfil their duties to maintain compliance.
- Taking an open approach to data protection to ensure staff, students and parents are comfortable raising any concerns. This is achieved by ensuring 'Privacy Notices' are accessible to all parties, regularly briefing individuals on key elements of data protection and displaying visual aids such as posters with key information around the school site.
- Training staff on data protection law, cyber security and providing regular briefings on this policy and related procedures on a routine basis.
- Integrating data protection into key policies and procedures and ensuring these are effectively communicated with relevant staff members.
- Conducting regular reviews and audits to test privacy measures and compliance with data protection law. This allows any gaps to be identified and improvement measures introduced where necessary. This includes retaining a log of data breaches.
- Completing DPIA's on data processing activities that may result in a high risk to the rights and freedoms of the individuals whose data we process.
- Maintaining an up to date 'record of processing activities' that outlines the type of data processed, 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.

20. Personal Data Breaches

The school make all reasonable endeavours to ensure that personal data breaches do not occur, we do however understand that gaps can occur in even the securest of systems. The school has therefore implemented a data breach procedure that clearly instructs staff to report breaches of any kind directly to the DPO.

The DPO will perform a review of the breach to ascertain the risks to the affected individuals' rights and freedoms. When appropriate, the DPO will report the data breach to the ICO within 72 hours and inform data subjects without undue delay.

A log of all data breaches is kept by the school and reviewed on an annual basis as a method to improve data security; staff are also encouraged to report 'near misses' as part of the data breach procedure.

21. Training

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continual professional development, where changes to legislation, guidance or the school's processes make it necessary.

In addition to data protection training, the school delivers briefings where necessary on key areas of this policy.

The school retain a log of training records.

22. Monitoring

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed every 3years or sooner if any fundamental change in legislation occurs. The policy will be reviewed and shared with the full governing board.

23. Linked Policies

This data protection policy is linked to our:

- Freedom of information Policy & Publication Scheme
- Acceptable Use Policy
- Online Safety Policy
- Safeguarding Policy
- Records Management Policy & Retention Schedule
- CCTV Policy
- Biometric Data Policy

24. Complaints

We ask that any concerns regarding this policy are made to the school in the first instance to allow us the opportunity to resolve your complaint. Individuals also have the right to complaint to the ICO if they feel the school is not processing personal data in compliance with data protection legislation:

Information Commissioners Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline: 0303 123 1113

Website: https://www.ico.org.uk

Appendix 1: Key Data Protection Terms

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 • Assessment records • Employment records 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.