



STAFFORD GRAMMAR SCHOOL

Prep 3-11 | Senior 11-16 | Sixth Form 16-19

Data Protection Policy

Policy Review

Date of Review	Reason for Review	Reviewer	Checked & approved	Date of approval	Next review
01.09.25	Annual review	Director of Finance & Operations	Headmaster	01.09.25	01.09.26

1. Introduction

During the course of Stafford Grammar School's (the "School") activities, personal data/information will be collected, stored and processed, including some sensitive personal information concerning its pupils and employees to enable it to function. The School recognises that it has a duty to comply with the UK GDPR and Data Protection Act 2018 (DPA) when handling personal information, and has implemented appropriate measures to do so. Correct and lawful treatment of this data will maintain confidence in the organisation, reduce risks to both the Data Subjects and the School, and will provide for successful business operations.

The School also recognises that it is required to notify the Information Commissioner's Office (ICO) concerning the personal information it processes, and when any alterations are made. This notification is publicly available on the ICO's website.

This policy sets out our approach to protecting data, and provides guidance for staff on how to deal with any personal information which they handle or are responsible for. It applies to all employees (including temporary staff) and Governors of the School. This policy covers all personal information created or held by the School regardless of whether this is in paper or electronic format.

On accepting the offer of a place at our School for their child, parents or guardians consent to the School obtaining, using, and holding personal information, including sensitive personal data about themselves and their child or children.

The DPA applies to all personal information of identifiable living individuals. Proof of death will be required for any subject access requests from relatives of the recently deceased.

2. Data Protection Principles

Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the general data protection regime. These are that personal data shall be:

- (i) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
- (ii) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
- (iii) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- (iv) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- (v) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
- (vi) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'); and
- (vii) the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

The DPA aims to allow organisations to maintain an appropriate balance between using personal information responsibly and respecting an individual's right to privacy.

3. Key Definitions

3.1 Data Controller

The individual, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. This may nominally be “the School”, which is interchangeable with a named individual(s), the School governors or the senior leadership team.

3.2 Data Processors

Data Processors act on behalf of, and only on the instructions of, the relevant Data Controller for the purposes of Processing that Data Controller's Personal Data. A data processor is anyone (other than an employee of the data). Data controllers will be responsible under the DPA for all processing carried out by their data processors.

3.3 Processing

This is a broad term and it covers obtaining, recording, organising, using, disclosing, deleting and holding data. In short, anything done to or with personal information is processing.

3.4 Personal data

Any information relating to an identifiable living individual (Data Subject); i.e. can be identified directly or indirectly, for example by an identifier such as name, pupil number, location data, an online identifier and/or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Specific examples include names of employees and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments and staff development reviews held in structured filing systems.

In addition to letters, emails, and documents held in files and folders, personal data can also include:

- Photographs and video recordings (including CCTV)
- Some SMS texts and voicemails
- Some minutes of meetings

3.5 Data Protection Officer (DPO)

The DPO assists the School to operate in compliance with Data Protection Legislation by improving accountability, providing advice and helping to monitor compliance. The DPO for the School will be the Director of Finance & Operations. They help implement the requirements of Data Protection Legislation across the School such as:

- i. The principles of data processing
- ii. Data Subjects' rights and complaints
- iii. Data protection by design and by default
- iv. Records of processing activities
- v. Security of processing
- vi. Notification and communication of data breaches

4. Responsibilities

4.1 This policy is monitored by the DPO. They are responsible for:

- Ensuring this policy is regularly reviewed, updated and implemented.
Ensuring the School's registration with the Information Commissioner's Office is reviewed and renewed regularly.
- Ensuring that any subject access requests are dealt with efficiently.
- Providing advice concerning information management to their employees as required, including arranging any additional training or written guidance.

4.2 The School's employees are responsible for:

- Ensuring that they are aware of this policy and accept their responsibility for complying with it when they come into contact with personal data.
- Requesting clarification as required with any aspects of this policy, or requesting additional training.

5. Security of Personal Information

We take the security of the personal data which we hold very seriously, and all employees and Governors must understand the importance of ensuring that personal data is secure.

Data controllers must take appropriate "technical and organisational measures" to ensure the security of the personal data they process – this means not only ensuring that the personal data is not stolen or accessed by inappropriate people, but also ensuring that the data is not accidentally lost, damaged or destroyed.

This section of the policy sets out the steps which our employees and Governors are expected to take in order to ensure that the School complies with the DPA.

5.1 Entry controls and paper records

Personal data must only be managed by employees of the School. Any member of staff witnessing unauthorised access or who has reason to query a given explanation is obliged to report it to a member of the Senior Leadership Team. The following must always occur:

- Paper records containing personal data must be kept securely in the School's offices.
- Paper files which are no longer required should be disposed of either by shredding or by secure arrangement with the maintenance team.
- Paper files sent by post must always be delivered by a registered courier.

5.2 Electronic Records

- Pupil personal data which has been collected since the introduction of SIMS is stored on the secure database which is password protected and has a sliding scale of access and control levels.
- Staff must not share their passwords. Passwords are strongly advised to be a combination of numbers and letters and include at least one special character. Passwords such as dates of birth or names of the user should be avoided. Staff are advised to regularly update their passwords.
- It is recommended that all laptops, memory sticks and portable devices are also encrypted with a strong password. It is not advisable for passwords to be the same across all devices used by a member of staff.
- Where email is used to contact groups of parents such as circular emails, these must be sent bcc (blind carbon copy) so that email addresses are not disclosed to everyone.
- In the reception or other public areas, employees must ensure that documents, including those on computer screens, are not visible to those who do not have the right to view them.

6. Personal Data Processed by the School

This section outlines the key groups about whom we hold and process personal information, including sensitive personal information.

6.1 Employees (including unsuccessful applicants for employment)

We hold data on all current employees. On the appointment of an applicant, the School will retain any relevant information provided on their application form (together with any attachments) on their personnel file.

If an applicant is unsuccessful, all documentation relating to the application will normally be confidentially destroyed after 6 months unless the applicant specifically requests the School to keep their details on file.

This information may include some or all of the following:

- Name
- Date of birth
- Current address (and previous address if the person has lived at their current address for less than 5 years), telephone and email address
- Next of kin/emergency contact
- Copies of identification documents such as passport or driving licence

- Disciplinary records
- Application for employment
- Details of CRB/DBS checks
- Performance management records including CPD
- Qualifications, including any copies of certificates made
- Sickness, on-going health conditions or extended periods of leave
- Details of previous employment, references, proof of right to work in the U.K., National Insurance number
- Ethnic background and religion
- Details of salary, bank details, expenses, deductions (e.g. student loan, childcare), pension payments
- Trade union or professional body membership
- Visual images

We keep this data to ensure we are able to make and evidence payments made (either as salary or pension contributions), communicate with employees, and evidence our compliance with legislation such as the Equality and Disability Discrimination Acts.

This information may be shared with others in our organisation if it is deemed directly relevant to the terms of their employment. We may also share information at the request of a named data subject, for example a former employee requiring a reference for new employment, or when required to disclose information by law.

6.2 Former Employees

We retain data concerning former employees for set periods of time to ensure we meet our legal requirements and for making pension payments/updating pension information.

This information is detailed in our retention schedule, but as a general rule we keep the following until the former employee is or would be aged 100, primarily for the administration of pensions:

- Full name and date of birth
- National Insurance number
- Written particulars of employment, including the formal contract
- Changes to terms and conditions, including change of hours letters
- Health declarations and medical assessments, including those relating to extended periods of leave and any documentation concerning an injury at work
- Copies of death certificate and/or marriage/civil partnership certificate (if applicable)
- Paperwork relating to periods of unpaid leave
- Personal payroll history, including record of pay, allowances, pay enhancements, other taxable allowances, reduced pay, no pay, maternity leave

- Pension estimates and awards
- Pensionable pay at leaving
- Reason for leaving and new employer's name (where known/applicable)
- Amount and date of any contributions
- Resignation, termination and/or retirement letters

We also keep records with shorter retention periods. Please see our Records Management Policy for further information on our retention policies.

6.3 Current and Former Pupils

We hold information concerning current pupils and former pupils until the pupil reaches the age of 25 years old. For pupils who attended the School prior to the use of digital /electronic records, their records are maintained in paper format and comprise of file covers with the following information on the cover: surname, forename, date of birth and SEN. SEN records require automatic retention for a longer period, see our Records Management Policy for further information on our retention policies.

Inside the front cover or maintained on SIMS (our current electronic pupil records system), we may also collect the following information:

- Emergency contact details
- The name of the pupil's doctor
- Gender
- Preferred name
- Position in family
- Language of home (if other than English)
- Religion
- Any allergies or other medical conditions that it is important for us to be aware of
- Names of parents and/or guardians with home address and telephone number (and any additional relevant carers and their relationship to the child)
- Name of previous school(s), the date of admission and the date of leaving.
- Attendance records
- Examination results
- Any other agency involvement e.g. speech and language therapist, paediatrician

6.4 Customers (Parents/Guardians/Fee Payers)

We rely on the financial contributions made as School fees to operate our daily business. We process and store personal and financial information in order to complete payments and maintain records of these regular transactions.

We keep records of sales made by the School for other services, such as transport, School visits, residential opportunities or other areas as required, together with information to support donations and associated Gift Aid claims.

We may hold any or all of the following information:

- Name and contact details of the bill payer
- Bank details, credit/debit card details, or other payment details such as when a payment was made, the total and reason for the payment
- The name(s) of pupil(s) which correspond to payments made
- The current balance owing

We keep this information to enable us to process payments and donations efficiently and to provide transaction trails in the event of a dispute.

6.5 Contractors, Suppliers, Professional Advisors

As part of our daily business, we seek and maintain contracts with external companies to help provide our core and extra-curricular functions. We hold personal information concerning current and recently terminated contracts, both relating to the company and details of contacts within the company.

We may hold any or all of the following information:

- Name and contact details of a contact within the company
- Bank details
- Records of payments made, copies of invoices
- Information relevant to the work being undertaken

We need this information to enable us to manage and administer our relationship with individual contractors and companies, including arranging for payment.

6.6 Complainants/Enquirers

Please see our Complaints Policy for full details of the records generated as part of this process. You may also wish to refer to The Education (Independent School Standards) (England) Regulations, 2010. To make a general enquiry, please refer to our website in the first instance, then if this does not answer your query, contact the School via the details enclosed later in this policy.

6.7 Individuals captured by CCTV images

The school is monitored by an in-house CCTV system. We use this as a deterrent for criminal activity. Recordings are regularly written over, usually on a monthly basis. Where necessary for identifying and prosecuting criminals, we share images with the police. All potentially identifiable subjects on our recordings are aware of CCTV recording through the use of several large signs around the School site.

7. Collecting Data

We recognise that we have a responsibility to collect information correctly and so the data collected is relevant for future use. It must be clear to the data subject (or their parent/guardian) why this information is being collected and what the School intends to do with the data. A sample copy of any form used to obtain data will be kept for as long as the data itself

We are required to meet at least one of the following conditions outlined in the DPA concerning the collection of personal data:

1. The individual has given his or her consent to the processing;
2. It is necessary for the legitimate interests of the Data Controller;
3. It is necessary for the performance of a contract relating to an individual;
4. It is necessary to ensure compliance with a legal obligation;
5. It is in the individual's vital interests (this usually means where it is a matter of life or death);
6. It involves the administration of justice (including a criminal investigation);
7. It is carried out in order to comply with legislation; or
8. It is in the substantive public interest, for the provision of confidential counselling, advice, support or any other service and is carried out without the individual's express consent because it is necessary where such consent cannot be given

8. Recording of Personal Information

Records are kept in such a way that the individual concerned or an external body (with appropriate access) can inspect them. To achieve this, the School should adhere to the following guidelines:

- Information stored must be correct, unbiased, unambiguous and legible if handwritten. Where information is obtained from an outside source, details of the source and date obtained should be recorded.
- Pupils/Parents or Guardians should have opportunities to provide updated information.
- Any person whose details, or child's details, are to be included on the School's website will be required to give written consent.

- With regards to photographs, the DPA may apply in certain circumstances. However, we take the matter extremely seriously and seek to obtain parents' permission for the use of photographs outside the School and, in particular, to record their wishes if they do not want photographs to be taken of their children.

9. Retention of Personal Information

Personal data should not be retained by an organisation for any longer than is necessary. This means that when personal data no longer needs to be retained by the School for any purpose it should be destroyed. Please refer to our Records Management Policy for further information on our retention policies.

9.1 Exceptions to the standard retention period

In exceptional circumstances, it may not be possible to implement the retention schedule as designed. Possible cases may include where personal information is:

- Relevant to legal action that has been started, or is threatened.
- Required to be kept by a contractual obligation or legislation.
- Being retained as a sample for statistical, research or historical purposes.

If in doubt, employees should seek advice from the Senior Management Team. Where records are being kept beyond the standard retention period, the records should be clearly marked and the reasons for the extension should be clearly identified. **It is not acceptable for this decision to be given verbally or based on a mutual understanding between current employees - it MUST be documented in writing.**

9.2 No Specified Retention Period

In the event of no retention period being specified, as a default the record should be retained for no more than 6 years after last being used (the usual period in which legal action can be brought following an event). The necessity of retaining the record should be kept under regular review, and if this is a record which is regularly created, used and stored it is recommended that the retention schedule be updated accordingly. If in doubt, it is always best practice to ask.

10. Provision of Data

It is a criminal offence to knowingly or recklessly obtain or disclose information about an individual without legitimate cause. Relevant, confidential data should only be given to:

- Employees and Governors of the School on a need-to-know basis.
- Parents/Guardians of the data subject, where they are under the age of 18.

- Schools to which a pupil may move, where there are legitimate requirements to do so (usually a request from a parent/guardian or the receiving school).

Other people we may share information more generally with include:

- Examining bodies
- Prospective employers of former employees
- Central and local government
- Healthcare professionals, social and welfare organisations
- Police, courts, tribunals and security organisations
- Voluntary and charitable bodies
- The media (images, names and ages)
- Suppliers
- Financial organisations
- Service providers
- Professional advisers
- The Independent Schools Inspectorate or other inspecting authorities, including the Secretary of State for Education.

The School will not disclose anything on a pupil's record which would be likely to cause serious harm to their physical or mental health or that of anyone else. When student records are created, this information is detachable from the main file.

If in doubt, staff must seek advice from the Senior Leadership Team. Where the Senior Leadership Team are unable to provide an adequate response, it is the responsibility of the Senior Leadership Team to seek out the appropriate answer from the next level of the hierarchy, ultimately ending with the Information Commissioner's Office.

The Independent Schools Inspectorate uses information about the progress and performance of pupils to help inspectors to periodically evaluate the work of our schools, to assist us in our self-evaluation, and as part of their assessment of the effectiveness of our educational initiatives and policy. Inspection reports do not identify individual pupils.

10.1 Providing of information in person

Where a request is made in person by a parent/guardian, their identity must be confirmed before access to information is granted. Suitable documents for confirming identity include:

- Passport
- Photographic Driving Licence
- Photographic ID card

Where photographic ID is not available, it may be possible to confirm identity using:

- Utility bill
- P45/P60
- Birth certificate
- Bank statement

(These lists are not exhaustive)

10.2 Provision of information via the telephone and email

The identity of the caller **MUST** be verified before issuing information over the telephone or by email. Questions should be asked to the individual, to which only they are likely to know the answers. This ensures information does not fall into the wrong hands, and keeps the pupils safe.

Where possible, personal information should not be disclosed using either method. If sending personal information by email, it is good practice to send this as an encrypted attachment, and send the password to the recipient using another method of communication.

Information should only be provided to those with parental responsibility for the pupil.

11. Exemptions from provision of data

The DPA identifies that certain data is exempt from the standard rights of access. This includes:

- Information which identifies other individuals and cannot be suitably redacted to remove these individuals. Where information can be redacted and a redacted copy is provided to the enquirer, a copy of this redacted information will be kept as evidence in the event of a complaint about the information provided.
- Information which the School reasonably believes will cause damage or distress. The exemption only applies to the extent that complying with the right of access would be likely to cause serious harm to the physical or mental health of any individual. This is known as the 'serious harm test' for education data.
- Data prepared for the prevention and detection of crime
 - Information required to be disclosed by law or in connection with legal proceedings
 - Disclosure prohibited or restricted by enactment, including personal data restricted by certain specific provisions of enactment covering special educational needs.

- Examination scripts written by a pupil. But it only applies to the information recorded by candidates. This means candidates do not have the right to copies of their answers to the exam questions. However, the information recorded by the person marking the exam is not exempt from the above provisions. If an individual makes a subject access request for this information before the results are announced, special rules apply to how long you have to comply with the request. You must provide the information:

(a) within five months of receiving the request; or

(b) within 40 days of announcing the exam results, if this is earlier.

- Data that does not concern a living individual

We also treat references provided to external bodies, including UCAS, CUKAS or any other academic body as part of an application for further or higher education, training or employment as confidential subject to meeting the conditions for disclosure below.

Where we hold a reference from an external source concerning a pupil or an employee, we may only disclose these references if both of the following conditions are met:

- The disclosure will not identify the source of the reference

- The referee has given consent

12. Subject Access Requests

Any person whose details are held by the School is entitled, under the DPA, to ask for a copy of all information held about them (or the child for whom they are responsible).

When a request is received it must be dealt with promptly; a response must be provided as soon as possible and within one month (A calendar month is calculated from the date the request is received to the corresponding date in the next month.). Requests for school records must be answered within 15 school days.

The School reserves the right to make a charge for a Subject Access Request where:

- **It is manifestly unfounded or excessive:** If a request is deemed clearly unreasonable, repetitive, or intended to disrupt the School, we will charge a reasonable fee (see below) to cover our administrative costs.
- **It is a request for further copies:** If you've already received a copy of your information and are requesting another, the School will charge a fee.

This fee will equate to £25.00 per hour per person (plus VAT if applicable) to cover staff time and associated costs.

12.1 What must a response to a Subject Access request contain?

- The requested information.
- A description of why the information is processed.
- Details of anyone it may be disclosed to.
- The source of the data.

Or, where there are insufficient grounds to disclose information, a written response outlining why the request has been refused, for example if the request has come from another individual rather than the data subject.

12.2 Provision of data to children

There is no definitive age at which a child must, can or should take responsibility for their own data.

The Information Commissioner's Office advises that by the age of 12 a child is generally expected to possess sufficient maturity to understand the nature of the request; however, this should be judged on a case-by-case basis.

If the child does not understand the nature of the request, a parent or a guardian is entitled to make the request on behalf of the child and receive a response.

13. Parents' rights

An adult with parental responsibility can access the information about their child, as long as the child is not considered to be sufficiently mature. If the child understands the request, they should be informed before a parent/guardian is granted access to the information and their views must be taken into account before a decision is made. We reserve the right to request appropriate documentation to evidence parental responsibility and to see identification from the requestor before the request is processed.

14. Complaints from Data Subjects

If an individual complains that the personal data held about them is wrong, incomplete or inaccurate, this should be investigated thoroughly including checking with the source of the information. In the meantime a caution should be marked on the person's file that there is a question mark over the accuracy.

Out of date information should be discarded if no longer relevant. Information should only be kept as long as needed, for legal or business purposes.

15. Contacting the School

This information can be found at the foot of all official correspondence and on our website. If you wish to write to the school, you can do so at:

Stafford Grammar School/Stafford Preparatory School
Burton Manor,
Stafford
ST18 9AT

Or you can contact us by:

Telephone: 01785 249752

Email: headsec@staffordgrammar.co.uk

If you wish to contact the School Governors, please use the above address and direct correspondence to Rev J Davis, Chair of Governors.

16. Policy Breaches

Ensuring compliance of the policy of all employees and Governors remains the responsibility of the DPO. It should be noted:

- Non-compliance may result in bad publicity and in some cases a large fine or prosecution which could be fundamentally damaging to the School's reputation and continued existence.
- Non-compliance by a member of staff is treated as a disciplinary matter which, depending on the severity or circumstances, could lead to dismissal.

17. Reporting a Personal Data breach

17.1 A data breach is an event or action resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data held and processed by the School.

17.2 The UK GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator (the Information Commissioner Office or ICO in the UK) and, in certain instances, the Data Subject. If a Data Breach is reportable to the ICO, the School must make that report within 72 hours of becoming aware of the breach.

17.3 Where the School is not the Data Controller and becomes aware of any Personal Data Breach relating to data that it holds and / or processes on behalf of another organisation, it is obligated to inform that organisation as soon as it becomes aware of the same.

17.4 In some cases, it may be determined that the affected Data Subjects should be notified of a Personal Data Breach, which will be determined by the Director of Finance and Operations.

17.5 All staff have a duty to notify the School's DPO of any confirmed or suspected Personal Data Breach. If staff know or suspect that a Personal Data Breach has occurred, they should immediately report the incident. Staff must retain all evidence relating to Personal Data Breaches to enable the School to maintain a record of such breaches, as required by the UK GDPR.

18. Related Policies

This policy is designed to be read alongside:

- The Safeguarding Policy
- The Complaints Procedure
- Records Management Policy
- Data Breach Policy
- Privacy Notices