DATA PROTECTION POLICY

Policy Status			
Policy Title	**Data Protection Policy**		
Author	Jonathan Yardley	Created	
		Updated	June 2024
Staff Responsibility	Admin & Planning Manager		
Review Period	1 year	Next Review	June 2025

STRATFORD UPON AVON SCHOOL

DATA PROTECTION POLICY

INTRODUCTION

Stratford upon Avon School collects and uses personal information about staff, students, parents and other individuals who come into contact with the school, in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information and share information with third parties in order to ensure the school complies with its statutory obligations.

Schools have a duty to be registered as data controllers with the Information Commissioner's Office (ICO), detailing the information held and its use. Schools also have a duty to provide a Privacy Notice to all staff, students, parents and carers, which summarises the information held, why it is held and the other parties to whom it may be passed on.

PURPOSE

This policy is intended to ensure that all staff involved with the collection, processing and disclosure of personal data will ensure personal information is dealt with correctly and securely and in accordance with the Data Protection Act 2018 and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

RELATED DOCUMENTS

This policy has due regard to the relevant legislation and statutory guidance including, but not limited to, the following**:**

- UK GDPR
- CCTV Policy
- SuAS Privacy Notice
- Freedom of Information Act 2000
- Data Protection Act 2018
- Data Security Breach Procedure
- FOI Publication Scheme
- ICT Network Acceptable Use Policy
- Protection of Freedoms Act 2012
- Records Management Policy and Retention Schedule
- Secure Desk Policy
- Subject Access Request Procedure
- SuAS Information Sharing Agreement
- SuAS Information Processing Agreement

1. Responsibilities

Data Controller (Stratford upon Avon School)

Has overall responsibility for compliance with the Data Protection Act 2018 and other related legislation.

Data Protection Lead - Administration & Planning Manager

As the Data Protection Lead, is responsible for creating and maintaining policies and procedures; registration with the Information Commissioners Office; Freedom of Information Requests and Subject Access Requests.

Data Protection Officer

The data protection officer (DPO) is responsible for providing advice and guidance to Stratford upon Avon School in order to assist the school to implement this policy, monitor compliance with data protection law, and develop related policies and guidelines where applicable.

The DPO will carry out an annual audit of the school's data processing activities and report their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO is the School DPO Service and is contactable via schooldpo@warwickshire.gov.uk or alternatively;

School Data Protection Officer
Warwickshire Legal Services
Warwickshire County Council
Shire Hall
Market Square
Warwick
CV34 4RL

Governors

Have overall responsibility for compliance with the Data Protection Act 2018 and other related legislation.

Headteacher

Is responsible for ensuring compliance with the Data Protection Act 2018, other related legislation and this procedure within the day to day activities of the school and ensuring appropriate training is provided for all staff.

All members of staff, governors and third parties who hold or collect personal data

Are responsible for their own compliance with the Data Protection Act 2018 and other related legislation and must ensure that personal information is kept and processed in line with current legislation. Additionally, all staff are responsible for ensuring any information held about themselves is accurate and up to date.

Parents/Carers

Are responsible for ensuring any information held about themselves or their child(ren) is accurate and up to date.

2. Definitions

Data Subject

The identified or identifiable living individual to whom personal data relates.

Data Controller and Processor

As a general rule, the definitions of controller and processor according to current legislation are that

‘controller’ means the natural or legal person who alone or jointly with others determines the purpose and means of the processing of personal data and ‘processor’ means the natural or legal person who processes personal data on behalf of the controller.

Processing
In relation to information, means an operation or set of operations which is performed on information, or on sets of information, such as:

- Collection, recording, organisation, structuring or storage.
- Adaptation or alteration
- Retrieval, consultation or use
- Disclosure by transmission, dissemination or otherwise making available.
- Alignment or combination.
- Restriction, erasure or destruction.

Consent
Consent must be a positive indication expressly confirmed in words. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual’s wishes

Personal Data Breach
The term ‘personal data breach’ refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Filing System
Any structured set of personal data which is accessible according to specific criteria, whether held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographical basis.

3. Applicable Data

Personal data
For the purpose of this policy, ‘personal data’ refers to information relating to an identified or identifiable living individual. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

Identifiable living individual
A living individual who can be identified, directly or indirectly, in particular by reference to:

- An identifier such as a name, an identification number, location data (incl. IP address) or an online identifier; or
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Special Categories of personal data

- Genetic data
- Biometric data
- Data concerning health
- Data concerning a natural person’s sex life or sexual orientation
- Personal data which reveals:
- Racial or ethnic origin.
- Political opinions
- Religious or philosophical beliefs
- Trade union membership

4. Data Protection Principles

In accordance with the requirements outlined in the UK GDPR, personal data will be processed according to the following six principles:

1. **Lawfulness, fairness and transparency.**
   Processing must be lawful, fair and transparent.

2. **Purpose limitation.**
   Purposes of processing must be specified, explicit and legitimate.

3. **Data minimisation.**
   Personal data must be adequate, relevant and not excessive.

4. **Accuracy.**
   Personal data must be accurate and kept up to date.

5. **Storage limitation.**
   Personal data must be kept for no longer than is necessary.

6. **Integrity and confidentiality.**
   Personal data must be processed in a secure manner.

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

5. Accountability

The UK GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with" the above principles (referred to as the accountability principle). The school will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR, and will provide comprehensive, clear and transparent privacy policies.

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

The school will also document other aspects of compliance with the UK GDPR and DPA where this is deemed appropriate in certain circumstances by the DPO, including the following:

- Information required for privacy notices, e.g. the lawful basis for the processing
- Records of consent
- Controller-processor contracts
- The location of personal data
- Data Protection Impact Assessment (DPIA) reports
- Records of personal data breaches

The school will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Minimising the processing of personal data.
- Pseudonymising personal data as soon as possible.
- Ensuring transparency in respect of the functions and processing of personal data.
- Continuously creating and improving security features.

6. Collecting Personal Data

6.1 Lawfulness, Fairness and Transparency

The legal basis for processing data will be identified and documented prior to data being processed. Under the UK GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained
- Processing is necessary for a contract held with the individual, or because they have asked the school to take specific steps before entering into a contract
- Processing is necessary for compliance with a legal obligation (not including contractual obligations)
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for protecting vital interests of a data subject or another person, i.e. to protect someone's life
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject – this condition is not available to processing undertaken by the school in the performance of its tasks

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- Processing relates to personal data manifestly made public by the data subject
- Processing is necessary for:
    - Carrying out obligations under employment, social security or social protection law, or a collective agreement
    - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
    - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
    - Reasons of substantial public interest with a basis in law which is proportionate to the aim pursued and which contains appropriate safeguards
    - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services with a basis in law
    - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices

- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with a basis in law

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

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

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law. We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

The school therefore has privacy notices for the following groups, which outline the information above that is specific to them:

- **Prospective employees**
- **Pupils and their families**
- **School workforce**

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary. Staff must only process personal data where it is necessary in order to do their jobs. We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

7. Consent

Consent can be withdrawn by the individual at any time by emailing admin@stratfordschool.co.uk. Where consent is given, a record will be kept documenting how and when consent was given.

The school ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

When pupils and staff join the school, the staff member or pupil (or, where appropriate, pupil's parent/carer) will be required to complete a consent form for personal data use. This consent form deals with the taking and use of photographs and videos, amongst other things. Where appropriate, third parties may also be required to compete a consent form.

Where the school opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined above, the school may, where appropriate, obtain consent directly from that child; otherwise, consent is obtained from whoever holds parental

responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children. In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the school on a case-by-case basis, taking into account the requirements outlined above.

8. Data Protection Rights of the Individual

Individuals have the following rights in relation to the handling of their data:

- To obtain a copy of their personal data as well as other supplementary information, including confirmation that their data is being processed, and the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing
- Withdraw their consent to processing at any time, where processing is based on the consent of the pupil or parent
- 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
- Object to processing which has been justified on the basis of public task, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

9. Subject Access Requests

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

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

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

- Name of individual
- Name of School
- Correspondence address

- Contact number and email address
- Details of the information requested

The DPO will send the subject access request to the Data Protection Lead. If staff receive a subject access request, they must immediately forward it to the Data Protection Lead. Subject Access Requests are handled in accordance with the **Subject Access Request Procedure**.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the person should have parental responsibility for the child, and 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, subject access requests from parents or carers of pupils at our school aged 13 and above may not be granted without the express permission of the pupil.

Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from parents or carers of pupils at our school [aged under 13] will in general be granted without requiring the express permission of the pupil.

These are not fixed rules and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to Subject Access Requests

When responding to requests, we:

- Will ask the individual to provide a form of photo 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 unless an extension is needed where a request is either complex or numerous
- Will provide the information free of charge

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Would include another person's personal data that we can't reasonably anonymise
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee 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 or they can seek to enforce their subject access right through the courts.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Biometric recognition systems

The school 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 pupils have the right to choose not to use the school biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils 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 pupil 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 pupil'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 school will delete any relevant data already captured.

12. CCTV

The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. We will adhere to the ICO's guidance for the use of CCTV. We use CCTV in various locations around the school site for security purposes. Footage is retained for 30 days and is deleted on a rolling basis. We may keep data for longer where we are required to review footage for an investigation. In such a case we will delete the footage once we no longer need it and in line with our retention schedule.

The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

Our lawful basis for using CCTV is legitimate interest. 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 and how you can contact us if you have any queries relating to the use of CCTV on our premises.

We have undertaken a data protection impact assessment in relation to our CCTV system to comply with our legal obligations. Our assessment is reviewed every two years.

13. Photographs and videos

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

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

The school will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way, unless we have consent, we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

14. Data protection by design and default

The school shall put measures in place to show that it has integrated data protection into all of its 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).
- Consideration of whether a data protection impact assessment needs to be undertaken. The school will consider this if any of the following kinds of processing plan to be undertaken:
    - Use of systematic and extensive automated processing
    - Large scale processing of data, particularly where it involves special category or criminal offence data
    - Systematic monitoring of publicly accessible areas and any other form of surveillance
    - Processing of biometric or genetic data
    - Transfer of data outside of the European Economic Area
    - Profiling, evaluation or scoring
    - Automated decision making with legal or significant effects
    - Matching or combining datasets
    - Processing of data concerning vulnerable data subjects
    - Implementation of new technology or solutions
    - If processing would prevent a data subject from exercising a right or using a service or contract

  On reviewing these criteria, if the school finds that the processing personal data presents a high risk to the rights and freedoms of individuals we will undertake a data protection impact assessment.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.

- Training members of staff on data protection matters
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO/DPL 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

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Staff must ensure passwords include numbers, a mix of upper and lower case and special characters
- Encryption software is used to protect all portable devices and removable media on which personal information is stored, such as laptops and USB devices.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment.
- 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.
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients. When sending confidential information staff will always check that the recipient is correct before sending.

16. Cloud computing

For the purposes of this policy, **'cloud computing'** refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the school accessing a shared pool of ICT services remotely via a private network or the internet.

As with files on school devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the school should unauthorised access, deletion or modification occur, and ensure ongoing compliance with the school's policies for the use of cloud computing.

The school's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the Data Protection Lead. The Data Protection Lead will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services.

The DPL will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.
- Ensure that the service provider can delete all copies of personal data within a timescale in line with the school's Data Protection Policy.
- Confirm that the service provider will remove all copies of data, including back-ups, if requested.
- Find out what will happen to personal data should the school decide to withdraw from the cloud service in the future.
- Assess the level of risk regarding network connectivity and make an informed decision as to whether the school is prepared to accept that risk.
- Monitor the use of the school's cloud service, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported.

17. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, the school will shred paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. Personal data breaches

The school shall take all reasonable steps to ensure that there are no personal data breaches. The school will ensure that all staff are made aware of, and understand, what constitutes a data breach as part of their training.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

When appropriate, the school shall report the data breach to the ICO within 72 hours. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed, and the individuals concerned will be contacted directly.

19. Training

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