South Staffordshire Learning Partnership

Data Protection Policy (GDPR)

Opening statement

South Staffordshire Learning Partnership (Bilbrook CofE Middle School, Codsall Community High School, Lane Green First School, Perton Middle School, St Chads CofE First School) is committed to complying with data protection legislation. This includes the UK version of the General Data Protection Regulation 2016, the Data Protection Act 2018 and the Privacy and Electronic Communication Regulations 2003.

This policy sets out the Partnerships approach (primarily through its employees and stakeholders) to the handling of personal data.

As a Partnership we recognise that the correct and lawful treatment of all stakeholders personal data will maintain their confidence in us and will provide for successful relationships.

Protecting the personal data of individuals is something that all the schools takes extremely seriously. It is of particular importance now that data is stored electronically and available to all staff who are homeworking as part of our new ways of working. Anyone who processes personal data on behalf of any of our schools such as students, employees, governors, contractors and suppliers must comply with this policy.

Compliance with this policy is mandatory. Related policies and procedures/guidelines are available to assist all stakeholders in complying with legislation including a Document Retention Policy. Any breach of this policy or the related policies and procedures/guidelines may result in disciplinary action, termination of contracts or action under the Partnerships Code of Conduct.

Review Officer - Mr N Eveson
Review Date – September 2025

Why does the Partnership need a Data Protection Policy?

The Partnership Governing Board has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Executive Head Teacher and Governors intend to comply fully with the requirements and principles of the Data Protection Act 1998 and the General Data Protection Regulation which came into force May 25th 2018.

All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines. By following the procedure, the Partnership will fulfil its obligations under the act.

Scope

An essential activity within the Partnership is the requirement to gather and process information about its staff and pupils in order to operate effectively.
This will be done in accordance with the Data Protection Act 2018 and other government legislation. This includes:

- The Freedom of Information Act 2000;
- GDPR may 2018
- The Human Rights Act 1998;
- Regulatory Investigation Powers Act 2000;
- 1990 Computer Misuse Act;
- Telecommunication Regulations Act1999 (Data Protection & Privacy);
- Crime and Disorder Act 1998.

1. Aims

The Partnership aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the Data Protection Act 2018.
This policy applies to all data, regardless of whether it is in paper or electronic format.

The Partnership will ensure that the Information Commissioners Office is informed of all its uses of information, and will conduct periodic reviews and update those entries.

The 2018 Act places a strong legal duty on the Data Controller (The Schools) to comply with the Act. To this end, the Partnership has adopted the policy as specified below. The individual Schools, acting as custodians of personal data, recognize their moral duty to ensure that it is handled properly and confidentially at all times, irrespective of whether it is held on paper or electronic means. This covers the whole lifecycle, including:

- the obtaining of personal data;
- the storage and security of personal data;
- the use of personal data;
- the disposal/destruction of personal data.

The Partnership also has a responsibility to ensure that data subjects have appropriate access upon written request to details regarding personal information about them.

2. Legislation and Guidance

This policy meets the requirements of the Data Protection Act 2018, and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education. It also takes into account the expected provisions of the General Data Protection Regulation, which is new legislation and came into force in May 2018.

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

3. Definitions

Personal data

Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified

Special category personal data

- Contact details
- Racial or ethnic origin
- Political opinions
- Religious beliefs, or beliefs of a similar nature
- Where a person is a member of a trade union
- Physical and mental health
- Sexual orientation
- Whether a person has committed, or is alleged to have committed, an offence
- Criminal convictions
- membership of a trade union
- their genetic/biometric data (if used to identify them)

Processing
Obtaining, recording or holding data. includes receiving information, storing it, considering it, sharing it, destroying it etc.

Data subject
The person whose personal data is held or processed.

Data controller
A person or organisation that determines the purposes for which, and the manner in which, personal data is processed.

Data processor
A person, other than an employee of the data controller, who processes the data on behalf of the data controller.

Consent
means any freely given, specific, informed and unambiguous indication of a person's wishes by which he/she/they/them, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

Pseudonymisation
Pseudonymisation is where any identifiable data is substituted with non-identifiable data in such a way that additional information is then required to re-identify the data subject.

Third Party A person or organisation other than the school/academy.

4. The Data Controller & Data Processor

The schools process personal information relating to pupils, staff and visitors, and, therefore, is a data controller. Each school delegates the responsibility of data controller to the Executive Head Teacher. The schools are registered as a data controller with the Information Commissioner's Office and renews this registration.

Our Data Protection Officer is care of Staffordshire County Council.

5. Data Protection Principles

The Data Protection Act 2018 is based on the following data protection principles, or rules for good data handling:

- Lawfulness, fairness and transparency

- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

6. The Schools MUST:

(a) process personal data fairly, transparently and only if there is a legal basis to do so.

To comply with this, employees must provide individuals when collecting their personal data (concisely and using clear and plain language so that they understand) with the following information:

1. that the Partnership is the "controller" of their personal data;
2. the Partnerships contact details;
3. why the Partnership is processing their personal data and in what way the law allows it;
4. if the Partnership [this will be rare] relies on its 'legitimate interests' or those of a third party for processing personal data what those interests are;
5. the identity of any person/ organisation to whom their personal data may be disclosed;
6. whether it is intended to process their personal data outside the United Kingdom;
7. how long their personal data will be retained for; and,
8. their rights. Privacy information should be tailored to the recipient so that they clearly understand what is happening with their data and their rights.

(b) only collect personal data for specified, explicit and legitimate purposes.

Employees must not further process any personal data in a manner that is incompatible with the original purposes; Employees should be clear as to what the Partnership will do with a person's personal data and only use it in a way they would reasonably expect.

(c) ensure that the personal data it collects is adequate, relevant and limited to what is necessary to carry out the purpose(s) it was obtained for;

Employees should think about what the Partnership is trying to achieve in collecting personal data. Employees must only collect the personal data that they need to fulfil that purpose(s) and no more. Employees must ensure that any personal data collected is adequate and relevant to the intended purpose(s).

(d) ensure that the personal data it processes is accurate and, where necessary, kept up to date.

Employees must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Employees must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

7. Data Integrity

The Partnership undertakes to ensure data integrity by the following methods:

Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs a School of a change of circumstances their computer record will be updated as soon as is practicable. A digital copy of their data record will be available they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the Schools will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

Examples of data would be pupil information on address, family details, free school meals etc., and school staff personnel details.

The Data Protection Officer will decide how long this information is kept and controlled for following Staffordshire County Council procedures and recommendations.

Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the schools to ensure that obsolete data are properly erased.

(This is linked to the DfE Retention Schedule of Records Management and advised by Staffordshire CC).

8. Authorized Disclosures

The Partnership will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the Partnership authorized officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations;
- pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare;
- pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school;
- staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters;
- unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the school. Officers and IT personnel writing on behalf of the LEA are IT liaison/data processing officers, for example in the LEA, are contractually bound not to disclose personal data.
- only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and pastoral officers will only be made available where the person requesting the information is a professional legitimately working within the school who need to know the information in order to do their work. The school will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.

A "legal disclosure" is the release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.

An "illegal disclosure" is the release of information to someone who does not need it, or has no right to it, or one which falls outside the School's registered purposes.

9. Data and Computer Security

The Partnership undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed):

Physical Security

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the control room. Printouts and other information areas (Hard drives) are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied. Passwords are used at all times and computers kept locked when not in the room.

Logical Security

Please see ICT security policy.

Procedural Security

In order to be given authorized access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents must be shredded before disposal.

Storing Personal Information

Overall security policy for data is determined by the Data Protection Officer and the Governing board and monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. The Partnership security policy is kept in a safe place at all times. Any queries or concerns about security of data in the school should in the first instance be referred to Mr. Neil Eveson.

Suspected breach

If I suspect that data has been accessed unlawfully, the Director of Business & Finance will inform the relevant parties immediately and report to the Information Commissioner's Office within 24 hours if necessary. The Partnership will keep a record of any data breach. All Data breaches must be reported to Network Manager or equivalent within 24 hours to secure the data if possible and to decide if the ICO need to be informed.

10. Roles and Responsibilities

The Governing board has overall responsibility for ensuring that the Partnership complies with its obligations under the Data Protection Act 2018.

Day-to-day responsibilities rest with the Director of Business & Finance as well as the appointed Data Protection Officer. The Data Controller will ensure that all staff are aware of

their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.

11. Privacy/Fair Processing Notice

11.1 Pupils and Parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the schools are performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on pupil characteristics, such as ethnic group or special educational needs
- Exclusion information
- Details of any medical conditions

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected. We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so.

We are required, by law, to pass certain information about pupils to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices- transparency-and-control/

** 10.2 Staff*

We process data relating to those we employ to work at, or otherwise engage to work at, our schools. The purpose of processing this data is to assist in the running of each school, including to:

- Enable individuals to be paid

- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Support the work of the School Teachers' Review Body

Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected. We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the school holds should contact the Director of Business & Finance.

12. Subject Access Requests

Under the Data Protection Act 2018, pupils have a right to request access to information the school holds about them. This is known as a subject access request.

Subject access requests should be submitted to Bal Dhaliwal . Requests should include:

- The pupils name
- A correspondence address
- A contact number and email address
- Details about the information requested

The schools will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child

Subject access requests for all or part of the pupils educational record will be provided within 1 calendar month

13. Data Access Requests

Requests for access must be made in writing. Pupils, parents or staff may ask for a Data Subject Access form, available from the Schools Administration Office. Completed forms should be submitted to Mr Neil Eveson. Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Pupil Record, Personnel Record), and the planned date of supplying the information (normally not more than 1 calendar month from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided. Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school dates in accordance with the current Education (Pupil Information) Regulations.

Parents have the right of access to their child's educational record, free of charge, within 15 school days of a request.

Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights. For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 13 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our school may be granted without the express permission of the pupil.

13.1 Other Schools

If a pupil transfers from the Partnership to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

13.2 Examination authorities

This may be for registration purposes, to allow the pupils at our schools to sit examinations set by external exam bodies.

13.3 Health Authorities

As obliged under health legislation, the schools may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

13.4 Police and Courts

If a situation arises where a criminal investigation is being carried out, we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

13.5 Social Workers and Support Agencies

In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

13.6 DfE and County

Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

13.8 Right to be Forgotten

Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

14. Storage of Records & Data Security

14.1 Storage of Records

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key and/or encryption password protection when not in use;
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access;
- Passwords must be changed in line with the schools IT security policy
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices;
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment.

14.2 Disposal of Records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely.
For example, we will shred or incinerate paper-based records, and override electronic files. We also use an outside company to safely dispose of electronic records using industry standard shredding.

14.3 Photographs and Video

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only.
Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources.
It is the school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

15. Criminal offence data

To process personal data about criminal convictions or offences, the Council must have a lawful basis under article 6 (above) and legal authority or official authority. For further advice speak with the Data Protection Officer.

16. Data protection rights

Individuals have rights when it comes to how the council handles their personal data. These include rights to:
a. withdraw consent to processing at any time;

b. receive certain information when the council collects their information or receives it from a third party;
c. request access to their personal data;
d. have the council correct inaccurate information;
e. ask the council to erase their personal data;
f. restrict the way the council uses their information;
g. be notified about any recipients of their personal data when they have asked for rectification, erasure or restriction;
h. object to any processing undertaken by the council in the public interest/exercise of official authority or its legitimate interests or those of another;
i. object to direct marketing by the council, and, to
j. be notified by the council of a personal data breach where it is likely to result in a "high risk" to their rights and freedoms.

Rights are not absolute. They are fact specific, and the council can say no to the request. They should normally be dealt with within a month of receipt and free of charge. Procedures exist (which should be followed) if a person seeks to exercise any of the above rights. If an employee receives a request by an individual to exercise a right the advice of the Data Protection Officer should be sought. Individuals can exercise their rights to access the information that the council holds about them by e-mailing their request to dpo@sstaffs.gov.uk

17. Training

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

Any employee deliberately acting outside of the recognized responsibilities may be subject to the council's disciplinary procedures, including dismissal where appropriate, and possible legal action.

18. The General Data Protection Regulation

We acknowledge that the law has changed on the rights of data subjects and that the General Data Protection Regulation has come into force in May 2018.

The links to all stakeholders we share or obtain data from are listed on our website.

19. Monitoring arrangements

The Partnership Director of Business & Finance is responsible for monitoring and reviewing this policy. The Director of Business & Finance along with the Data Protection Officer checks

that the school complies with this policy by, among other things, reviewing school records annually.

This document will be reviewed every 2 years or when legislation changes.

At every review, the policy will be shared with the governing board.

20. Links with other policies

This data protection policy and privacy notice is linked to the freedom of information publication scheme.
This data protection policy has links with the IT Security policy

21. Information Commissioners Office

This is the external regulator for Data Protection. The UK's independent body to uphold information rights.

Date of Approval by Governing Body:

_____

Signed by Chair of Governors:

_____

Review Officer - Mr N Eveson
Review Date – September 2025

Review date:

August 2025

_____

Person(s) Responsible for Day to Day Management:

Data Protection Officer, Data protection deputy

_____

Person Responsible for Review
Director of Business & Finance