



Shustoke C of E Primary School

# Data Protection & GDPR Policy

2026

This policy should be read in conjunction with our:

- Child Protection and Safeguarding Policy
- Security of Information Policy
- Freedom of information policy
- E-Safety Policy
- Acceptable use of ICT
-



## Shustoke C of E Primary School

### 1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(GDPR\)](#) and the provisions of the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Bill](#).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

### 2. Legislation and guidance

**This policy meets the requirements of the:**

- UK General Data Protection Regulation (UK GDPR) - the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

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.

The school is registered with the Information Commissioner for holding and processing of personal data. The school has a duty to protect this information and to keep it up to date. The school is required to share some of the data with other agencies including Warwickshire County Council and the Department for Education. Please see our Privacy Notice for full details of how we use and share the above personal information.

Please note you have the right to withdraw or amend your consent for the sharing of personal information at any time, although we will need to have certain personal information to fulfil our legal duties. You can notify us of a withdrawal of or any changes to your consent in writing by contacting [admin3207@welearn365.com](mailto:admin3207@welearn365.com)



### 3. Definitions

<b>Term</b>	<b>Definition</b>
<b>Personal data</b>	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none"><li>• Name (including initials)</li><li>• Identification number</li><li>• Location data</li><li>• Online identifier, such as a username</li></ul> <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
<b>Special categories of personal data</b>	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"><li>• Racial or ethnic origin</li><li>• Political opinions</li><li>• Religious or philosophical beliefs</li><li>• Trade union membership</li><li>• Genetics</li><li>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li><li>• Health - physical or mental</li><li>• Sexual orientation</li></ul>
<b>Processing</b>	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
<b>Data subject</b>	<p>The identified or identifiable individual whose personal data is held or processed.</p>
<b>Data controller</b>	<p>A person or organisation that determines the purposes and the means of processing of personal data.</p>
<b>Data processor</b>	<p>A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.</p>
<b>Personal data breach</b>	<p>A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.</p>



## Shustoke C of E Primary School

### 4. The Data Controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

### 5. Roles and responsibilities

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

#### 5.1 Governing Body

The Governing Body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

#### 5.2 Data Protection Officer

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

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board 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.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Warwickshire Data Protection Officer Services and is contactable on 01926 412174, via [schooldpo@warwickshire.gov.uk](mailto:schooldpo@warwickshire.gov.uk), or alternatively:

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

#### 5.3 Headteacher, School Business Manager and Health and Safety Officer

The Headteacher acts as the representative of the data controller on a day-to-day basis.

The School Business Manager (Data Protection Lead, DPL) monitors compliance with the GDPR policy, gives advice to staff and logs any reported breaches.



## Shustoke C of E Primary School

The Health and Safety Officer reviews the level of security in school and gives advice to staff and the Governing Body.

### 5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the Data Protection Leads in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

### 6. Data protection principles

The UK GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure
- This policy sets out how the school aims to comply with these principles.

### 7. Collecting personal data

#### 7.1 Lawfulness, fairness and transparency

We will only process personal data where

- we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:



### Shustoke C of E Primary School

- the data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- the data needs to be processed so that the school can comply with a legal obligation
- the data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- the data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions
- the data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)
- the individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent
- for special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.
- if we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

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

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- 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 has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation



### Shustoke C of E Primary School

- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

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 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
- The data needs to be processed for reasons of substantial public interest as defined in legislation

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.

#### 7.2 Limitation, minimisation and accuracy

- We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
- If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.



## Shustoke C of E Primary School

- 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.
- When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

### 8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies - we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils - for example, IT companies. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
  - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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

Where we transfer personal data internationally, we will do so in accordance with data protection law.

### 9. Subject access requests and other rights of individuals

#### 9.1 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



## Shustoke C of E Primary School

- 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 either by letter to the school postal address or by email to the Data Controller ([admin3207@welearn365.com](mailto:admin3207@welearn365.com)). They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the Data Controller, who will ensure that the DPO is informed.

### 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 child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

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 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:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 working month of receipt of the request
- Will provide the information free of charge



### Shustoke C of E Primary School

- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

*We will not disclose 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*
- *Is contained in adoption or parental order records*
- *Is given to a court in proceedings concerning the child*
- *Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it*
- *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.*

#### 9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- 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 (decisions taken with no human involvement, that might negatively affect them)
- 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)



## Shustoke C of E Primary School

- Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

### 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. Photographs and videos

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

We will obtain written consent from parents/carers for photographs and videos to be taken of their child. These photos and videos may be used for communication, marketing and promotional materials, within school on notice boards and in school magazines, brochures, newsletters, etc. Also outside of school by external agencies such as the school photographer and newspapers. Also online on our school website or social media pages.

We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

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 apart from their first name, to ensure they cannot be identified.

See our Child protection and safeguarding policy for more information.



## Shustoke C of E Primary School

### 12. Data Protection Complaints

We are committed to handling your personal data in a way that is fair, transparent, and in accordance with the law. If you are unhappy with how we have handled your data, this process outlines how you can make a complaint.

#### **How to Make a Complaint**

If you have a concern about how your personal data has been handled, please contact our Data Protection Lead (DPL) or our Data Protection Officer (DPO). This gives us the opportunity to investigate and resolve the matter as quickly as possible.

There is no set format for making a data protection complaint. However, submitting your complaint in writing may help us to respond more promptly. Please direct your complaint to:

- School/Trust Data Protection Lead (DPL) email: [admin3207@welearn365.com](mailto:admin3207@welearn365.com)
- School/Trust Data Protection Officer (DPO): [schooldpo@warwickshire.gov.uk](mailto:schooldpo@warwickshire.gov.uk)

When you contact us, please provide as much detail as possible about your complaint. This will help us to understand the issue and investigate it thoroughly

#### **What to Expect from Us**

We will acknowledge receipt of your complaint within 30 days. We will, without undue delay, take appropriate steps to respond to your complaint, including making appropriate enquires.

Throughout the process, we will:

- Keep you informed of our progress.
- Request any additional information we may need from you in a timely and proportionate manner.
- Provide you with a clear and comprehensive outcome of our investigation.

#### **If You Remain Unhappy**

If you are not satisfied with the outcome of your complaint, or if you feel we have not handled it appropriately, you have the right to complain to the Information Commissioner's Office (ICO). The ICO is the UK's independent regulator for data protection and information rights.

For more information about the ICO and their complaints process, you can visit their website at [ico.org.uk](http://ico.org.uk).

### 13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge. This is currently fulfilled via a traded service provided by Warwickshire County Council Legal Services.



### Shustoke C of E Primary School

- 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
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our school and DPO 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



## Shustoke C of E Primary School

### 14. 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
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Staff must ensure passwords are hard for anyone else to guess by incorporating numbers and mixed case into it.
- 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 (see section 8)

### 15. 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, we will shred or incinerate 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.

### 16. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.



## Shustoke C of E Primary School

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

### 17. Training

Data protection will form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary. All staff and governors are provided with data protection training as part of their induction process, annual Safeguarding and Safety Update (every September), and any updates provided through Staff Meetings, Briefings and email communication.

Guidance will be issued via regular policy review and the school staff and volunteer handbook.

### 18. Monitoring arrangements

The Governing Body is responsible for monitoring and reviewing this policy on advice from the DPO. This policy will be reviewed and updated by the Governing Body every two years.



Shustoke C of E Primary School

## Appendix 1: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the School Business Manager who will inform the Headteacher (and where necessary the DPO) and record appropriately using the Group Call electronic system.

- The School Business Manager and Headteacher (and where necessary the DPO) will investigate the report, and determine whether a breach has occurred. To decide, they will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people
- The School Business Manager will alert the Headteacher and the chair of governors
- The School Business Manager will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The School Business Manager will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The School Business Manager and Headteacher will determine whether the breach must be reported to the DPO and/or ICO. If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO. This must be judged on a case-by-case basis. To decide, the School Business Manager/Headteacher/DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.

Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the DPO will set out:

A description of the nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach



## Shustoke C of E Primary School

- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals - for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
  - Records of all breaches will be stored on the school's Data Breach Log

The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

### Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

For example:

- Special category data (sensitive information) is accidentally made available via email to unauthorised individuals:
  - The sender must attempt to recall the email as soon as they become aware of the error
  - Members of staff who receive personal data sent in error must alert the sender and the DPL as soon as they become aware of the error
  - If the sender is unavailable or cannot recall the email for any reason, the DPL will ask the ICT department to recall it
  - In any cases where the recall is unsuccessful, the DPL will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
  - The DPL will request a written response from all the individuals who received the data, confirming that they have complied with this request
  - The DPL will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.



Shustoke C of E Primary School

## Appendix 2: Appropriate Policy Document

### 1. About this policy

The Data Protection Act 2018 sets out the requirement to have an appropriate policy document when processing special category data and criminal offence data.

To fulfil our duties and function as a school/trust, we need to process personal information that is listed within Schedule 1 of the Data Protection Act 2018. Most of the processing within Schedule 1 of the Data Protection Act 2018 is required to have an appropriate policy document in place.

This is the appropriate policy document for Shustoke C of E Primary School setting out how we will protect special categories of personal data and criminal convictions data.

### 1. Why we process Special Categories of Personal Data and Criminal Convictions Data

1.1 We process Special Categories of Personal Data and Criminal Convictions Data for the following purposes:

- 1.1.1 assessing an employee's fitness to work;
- 1.1.2 complying with health and safety obligations;
- 1.1.3 complying with the Equality Act 2010;
- 1.1.4 checking applicants' and employees' right to work in the UK;
- 1.1.5 verifying that candidates are suitable for employment or continued employment; and
- 1.1.6 To safeguard pupils, staff, and the community.
- 1.1.7 To support pupils, staff, and visitors who have a medical condition or disability.
- 1.1.8 To support pupils with special educational needs
- 1.1.9 To meet our legal and ethical duties for the provision of education.



Shustoke C of E Primary School

1.2 Where we process special categories of personal data and criminal convictions data, we will identify our lawful basis under both Article 6 and Article 9 of the UK GDPR and, where appropriate, identify the condition with schedule 1 that allows for the processing.

1.3 Processing subject to Schedule 1 of the Data Protection Act 2018:

Processing condition for Special Categories of Personal Data	Description of Processing
Schedule 1, Part 1 - Conditions relating to employment, social security and social protection.	<p>Processing data concerning health where we have a duty outlined under employment law.</p> <p>Processing data concerning criminal convictions under Article 10 of the UK GDPR where we have a duty under employment law for recruitment, discipline, and dismissal. To comply with statutory guidance for safer recruitment</p> <p>Processing information relating to Trade Union Membership to facilitate your right and preference to participate as a member of any trade union, and where there is industrial action that may impact the function of the school.</p>
Schedule 1, Part 2 - Substantial Public Interest Conditions	<p>Statutory etc. And Government Purposes:</p> <ul style="list-style-type: none"> <li>• Compliance with legal obligations and support the provision of education such as completing the school census, providing a common transfer file, to support pupils with medial conditions, to support pupils with special educational needs.</li> <li>• Compliance with legal obligations in connection with legal proceedings</li> </ul>



Shustoke C of E Primary School

	<ul style="list-style-type: none"><li>• We may also process criminal offence data under this condition.</li></ul>
	<p>Equality of Opportunity and Treatment</p> <ul style="list-style-type: none"><li>• To provide equal access to education</li><li>• Compliance with legislation such as the Equality Act 2010.</li><li>• To ensure equality of treatment.</li></ul>
	<p>Preventing and detecting unlawful acts</p> <ul style="list-style-type: none"><li>• To comply with our duty to safeguard pupils and the community.</li><li>• To reduce risk to pupils, staff and visitors.</li><li>• Sharing information with relevant and authorised agencies to support the prevention or investigations of unlawful acts.</li></ul>
	<p>Protecting the Public against Dishonesty</p> <ul style="list-style-type: none"><li>• Assisting other agencies in connection with regulatory requirements.</li><li>• To protect and safeguard pupils and the community.</li></ul>
	<p>Support for Individuals with a Disability or Medical Condition</p> <ul style="list-style-type: none"><li>• To ensure we keep pupils and staff safe.</li><li>• To ensure all pupils can access education and other services in school.</li><li>• To ensure our employees are properly supported and able to do their job.</li></ul>



Shustoke C of E Primary School

	<p>Counselling</p> <ul style="list-style-type: none"> <li>To allow for individuals to access confidential counselling services as arranged through occupational health or other support services.</li> </ul>
	<p>Safeguarding of Children and Individuals at risk</p> <ul style="list-style-type: none"> <li>To protect and safeguard pupils from physical and emotional harm, neglect, or abuse.</li> <li>To support the wellbeing of pupils at our school.</li> </ul>
	<p>Insurance</p> <ul style="list-style-type: none"> <li>To process data that is required for insurance purposes.</li> </ul>
	<p>Occupational Pensions</p> <ul style="list-style-type: none"> <li>To meet our legal obligation to provide a pension scheme for our workforce.</li> </ul>
<p>Schedule 1, Part 3 - Additional Conditions Relating to Criminal Convictions, etc.</p>	<p>We process data criminal offence data for the purposes of recruitment and employment vetting. We may also process criminal offence data to protect and safeguard pupils, staff, and the community.</p>

2. Personal data protection principles

2.1 The UK GDPR requires personal data to be processed in accordance with the six principles set out in Article 5(1). Article 5(2) requires controllers to be able to demonstrate compliance with Article 5(1).

2.2 We comply with the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:



## Shustoke C of E Primary School

- 2.2.1 Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);
- 2.2.2 collected only for specified, explicit and legitimate purposes (Purpose Limitation);
- 2.2.3 adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);
- 2.2.4 accurate and where necessary kept up to date (Accuracy);
- 2.2.5 not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation); and
- 2.2.6 Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

2.3 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

### 3. Compliance with data protection principles

#### 3.1 Lawfulness, fairness and transparency

Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

We will only Process Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. We can Process Special Categories of Personal Data and Criminal Convictions Data only if we have a legal ground for Processing and one of the specific Processing conditions relating to Special Categories of Personal Data or Criminal Convictions Data applies. We will identify and document the legal ground and specific Processing condition relied on for each Processing activity.

When collecting Special Categories of Personal Data and Criminal Convictions Data from Data Subjects, either directly from Data Subjects or indirectly (for example from a third party or publicly available source), we will provide Data Subjects with a Privacy Notice setting out all the information required by the UK GDPR which is concise, transparent, intelligible, easily accessible and in clear plain language which can be easily understood.

#### 3.2 Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. They must not be further Processed in any manner incompatible with those purposes.



## Shustoke C of E Primary School

We will only collect personal data for specified purposes and will inform Data Subjects what those purposes are in a published Privacy Notice. We will not use Personal Data for new, different, or incompatible purposes from those disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have consented where necessary.

### 3.3 Data minimisation

Personal Data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

We will only collect or disclose the minimum Personal Data required for the purpose for which the data is collected or disclosed. We will ensure that we do not collect excessive data and that the Personal Data collected is adequate and relevant for the intended purposes.

### 3.4 Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

We will ensure that the Personal Data we hold and use is accurate, complete, kept up to date, and relevant to the purpose for which it is collected by us. We check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

### 3.5 Storage limitation

We only keep Personal Data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where we have a legal obligation to do so. Once we no longer need Personal Data it shall be deleted or rendered permanently anonymous.

We maintain a Data Retention Policy and related procedures to ensure Personal Data is deleted after a reasonable time has elapsed for the purposes for which it was being held, unless we are legally required to retain that data for longer.

We will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

### 3.6 Security, integrity, confidentiality

Personal Data shall be 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.



## Shustoke C of E Primary School

We will implement and maintain reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of or damage to Personal Data.

### 3.7 Accountability principle

We are responsible for, and able to demonstrate compliance with these principles. Our DPO is responsible for ensuring that we are compliant with these principles. Any questions about this policy should be submitted to the DPO.

We will:

- 3.7.1 Ensure that records are kept of all Personal Data Processing activities, and that these are provided to the Information Commissioner on request.
- 3.7.2 Carry out a DPIA for any high-risk Personal Data Processing to understand how Processing may affect Data Subjects and consult the Information Commissioner if appropriate.
- 3.7.3 Ensure that a DPO is appointed to provide independent advice and monitoring of Personal Data handling, and that the DPO has access to report to the highest management level.
- 3.7.4 Have internal processes to ensure that Personal Data is only collected, used or handled in a way that is compliant with data protection law.

### 4. Controller's policies on retention and erasure of personal data

We take the security of Special Categories of Personal Data and Criminal Convictions Data very seriously. We have administrative, physical, and technical safeguards in place to protect Personal Data against unlawful or unauthorised Processing, or accidental loss or damage. We will ensure, where Special Categories of Personal Data or Criminal Convictions Data are Processed that:

- 4.1.1 The Processing is recorded, and the record sets out, where possible, a suitable time for the safe and permanent erasure of the different categories of data in accordance with our Data Retention Policy/the relevant retention schedules.
- 4.1.2 Where we no longer require Special Categories of Personal Data or Criminal Convictions Data for the purpose for which it was collected, we will delete it or render it permanently anonymous as soon as possible.
- 4.1.3 Where records are destroyed, we will ensure that they are safely and permanently disposed of.

Data Subjects receive a Privacy Notice setting out how their Personal Data will be handled when we first obtain their Personal Data, and this will include information on how we determine retention periods. The Privacy Notices are also available on the School website.



## Shustoke C of E Primary School

### 5. Review

5.1 This policy on Processing Special Categories of Personal Data and Criminal Convictions Data is reviewed annually.

5.2 The policy will be retained where we process Special Categories of Personal Data and Criminal Convictions Data and for a period of at least six months after we stop carrying out such processing.

5.3 A copy of this policy will be provided to the Information Commissioner on request and free of charge.

Dated: March 2026

Next review: March 2027

Further information:

For further information about our compliance with data protection law, please contact our Data Protection Lead, or our Data Protection Officer at the School DPO Service, Warwickshire Legal Service, Shire Hall, Warwick - Email [schooldpo@warwickshire.gov.uk](mailto:schooldpo@warwickshire.gov.uk) (when contacting our DPO, please state which school your query relates to).

Approved by: Miss M Wall - Headteacher

Date: March 2026

Next review due: March 2027