



## Hagley Primary School

# GDPR Data Protection Policy including Freedom of Information

**Date reviewed:** November 2024

**Date of next review:** November 2025

**Responsible member of staff:** Tina Rennie

**Signature:**

.....

*(Chair of governors)*

**Signature:**

.....

*(Head Teacher)*

The School is committed to being concise, clear and transparent about how it obtains and uses personal information.

Data Protection Legislation (defined below) is the law that protects personal privacy and upholds individual's rights. This policy is intended to ensure that personal information is dealt with properly and securely by the School and in accordance with the Data Protection Legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Our Data Protection Officer ("DPO") is Mrs Tina Rennie who is contactable at Hagley Primary School, Park Road, Hagley, DY9 0NS, 01562 883280, [office@hagleyprimary.worcs.sch.uk](mailto:office@hagleyprimary.worcs.sch.uk). Our DPO is responsible for monitoring the compliance of the School with the Data Protection Legislation and any queries in relation to this policy or data protection issues should be raised with the DPO. The school will also have a nominated Governor in relation to data protection issues.

## **Policy Objectives**

The School as the Data Controller will comply with its obligations under Data Protection Law.

All staff and users of data must have a general understanding of the law and understand how it may affect their decisions to make an informed judgement about how information is gathered, used and ultimately deleted. All staff and users of data at the school must comply with this policy.

## **Scope of the Policy**

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information.

The school collects a large amount of personal data every year including pupil records, staff records, names and addresses of parents as well as the many different types of data used by the school. In addition, the school may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies including ethnicity and religion.

## **The principles**

The principles set out in the Data Protection Legislation must be adhered to when processing personal data:

1. Personal data must be processed lawfully, fairly and in a transparent manner.
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed.
4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed.
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

## **Transfer Limitation**

Personal data shall not be transferred to a country outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Staff should contact the DPO if they require further assistance with a proposed transfer of personal data outside of the EEA.

## **Lawful Basis for processing personal information**

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

- 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 school.
- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the data controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party.
- The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient.
- Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first consented.
- A school will have the right to decline the request to delete data where there is a legal obligation to store and retain for a set period of time. This set period of time is detailed in the national data retention policy. The school must be transparent and detail all retained information and the purpose of the retention.

The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in the School's privacy notice.

## **Sensitive Personal Information**

Processing of sensitive personal information (known as 'special categories of personal data') is prohibited unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed by the school if:

- There is a lawful basis for doing so.
- One of the special conditions for processing sensitive personal information applies: (a) The individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
  - (b) The processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject.
  - (c) The processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent.
  - (d) The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim.
  - (e) The processing relates to personal data which are manifestly made public by the data subject.
  - (f) The processing is necessary for the establishment, exercise, or defence of legal claims.
  - (g) The processing is necessary for reasons of substantial public interest.
  - (h) The processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services.
  - (i) The processing is necessary for reasons of public interest in the area of public health.

The school's privacy notice(s) set out the types of personal information that it processes, what it is used for and the lawful basis for the processing.

### **Automated Decision Making**

If the School carries out automated decision making (including profiling) it will ensure that it has a lawful basis for the processing. Explicit consent will usually be required for automated decision making (unless it is authorised by law, or it is necessary for the performance of or entering into a contract).

Additional safeguards and restrictions apply in the case of solely automated decision-making, including profiling. The school will as soon as reasonably possible notify the data subject in writing that a decision has been taken based on solely automated processing and that the data subject may request the school to reconsider or take a new decision. If such a request is received staff must contact the DPO as the school must reply within one calendar month. This date does not allow for school closures.

### **Data Protection Impact Assessments (DPIA)**

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA will be carried out. The DPO will be involved in any DPIA undertaken by the school.

### **Documentation and records**

Written records of processing activities will be kept by the school including:

- The name(s) and details of individuals or roles that carry out the processing.
- The purposes of the processing
- A description of the categories of individuals and categories of personal data
- Categories of recipients of personal data
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.
- Retention schedules
- A description of technical and organisational security measures.

Records of processing of sensitive information are kept on:

- The relevant purposes for which the processing takes place, including why it is necessary for that purpose and
- The lawful basis for our processing

The school will conduct regular reviews (at least annually) of the personal information it processes and update its documentation accordingly. This may include:

- Carrying out information audits to find out what personal information is held.
- Talking to staff about their processing activities
- Reviewing policies, procedures, contracts, and agreements to address retention, security, and data sharing.

## **Privacy Notice**

The school will issue privacy notices as required, informing data subjects (or their parents) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the GDPR including the identity of the data controller and the DPO, how and why the School will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

The school will issue a minimum of two privacy notices, one for pupil information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes.

## **Purpose Limitation**

Personal data will be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

## **Data minimisation**

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

Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

The school will ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with a data retention schedule. This includes: requiring third parties to delete such data where applicable.

## **Individual Rights**

Data subjects have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed.

- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request.
- To have data corrected if it is inaccurate or incomplete.
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing.
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the school no longer need the personal information, but you require the data to establish, exercise or defend a legal claim.
- To restrict the processing of personal information temporarily where you do not think it is accurate (and the school are verifying whether it is accurate), or where you have objected to the processing (and the school are considering whether the school's legitimate grounds override your interests)
- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.
- To withdraw consent to processing at any time (if applicable)

### **Individual Responsibilities**

Staff or other users of data must:

- Only access the personal information that you have authority to access and only for authorised purposes.
- Only allow other staff to access personal information if they have appropriate authorisation.
- Only allow individuals who are not school staff to access personal information if you have specific authority to do so.
- Keep personal information secure (e.g. By complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the national retention policy).
- Not remove personal information, or devices containing personal information (or which can be used to access it) from the school's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device.
- Not store personal information on local drives or on personal devices that are used for work purposes.

### **DPO**

The school can appoint an existing employee to the role of DPO provided they meet the necessary requirements and have sufficient knowledge of data protection law. Our current DPO is stated above. The DPO will operate independently with the support from the ICO.

### **Information Security**

The school will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure. Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the school has implemented and maintains in accordance with the Data Protection Legislation.

Where the School uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

### **Storage and retention of personal information**

Personal data will be kept securely in accordance with the school's data protection obligations.

Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained.

### **CCTV and photography**

If the School uses CCTV systems, this will be in accordance with data protection principles. The school will indicate its intentions for taking videos and photographs and will obtain consent before publishing videos or photographs. This can be in the form of a paper or verbal consent in exceptional circumstances. This can be for the duration of the child's time at school or longer for marketing purposes. Both consent methods should state the reason for the use and the retention period.

### **Data breaches**

A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored.
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams.
- Blagging offences where information is obtained by deceiving the organisation which holds it

The school must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours if the breach is likely to result in a risk to the rights and freedoms of individuals. The school must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform the DPO immediately that a data breach is discovered. The DPO will work with the member of staff to complete an internal data breach form for evidence/record keeping.

### **Training**

The school will ensure that staff are adequately trained regarding their data protection responsibilities.

### **Consequences of a failure to comply**

The school takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the school and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the school's procedures and this action may result in dismissal for gross misconduct. If a non- employee or 3<sup>rd</sup> party organisation breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact the school's DPO.

## **Review of Policy**

This policy will be updated as necessary to reflect best practice or amendments made to the Data Protection Legislation.

## **The Supervisory Authority in the UK**

Please follow this link to the ICO's website (<https://ico.org.uk/>) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data etc.

## **Glossary**

**Data Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

**Data Subject:** a living, identified or identifiable individual about whom we hold personal data.

**Data Privacy Impact Assessment (DPIA):** tools and assessments used to identify and reduce risks of a data processing activity.

**Data Protection Legislation:** Data Protection Act 2018, GDPR and any Relevant Legislation.

**Data Protection Officer (DPO):** the person required to be appointed in public authorities under the GDPR.

**EEA:** the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

**GDPR:** General Data Protection Regulation ((EU) 2016/679).

**Personal data** is any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier.

**Processing** means anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure or destruction.

**Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

**Relevant Legislation:** The Freedom of Information Act 2000, The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016), The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004, The School Standards and Framework Act 1998 and ICO guidance

**Sensitive Personal Data:** information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal data relating to criminal offences and convictions.



# Appendix 1

## Privacy Notice

### Hagley Primary School

#### GDPR Privacy Notice for Pupils and Their Families

##### Who processes your information?

Hagley Primary School is the data controller of the personal information you provide to us. This means the school determines the purposes for which, and the manner in which, any personal data relating to pupils and their families is to be processed. Mrs Tina Rennie acts as a representative for the school with regard to its data controller responsibilities.

In some cases, your data will be outsourced to a third-party processor; however, this will only be done with your consent, unless the law requires the school to share your data. Where the school outsources data to a third-party processor, the same data protection standards that Hagley Primary School upholds are imposed on the processor.

Mrs Tina Rennie is the Data Protection Officer (DPO). Her role is to oversee and monitor the school's data protection procedures, and to ensure they are compliant with the GDPR. The DPO can be contacted on 01562 883280 or [office@hagleyprimary.worcs.sch.uk](mailto:office@hagleyprimary.worcs.sch.uk).

##### Why do we collect and use your information?

Hagley Primary School holds the legal right to collect and use personal data relating to pupils and their families, and we may also receive information regarding them from their previous school, LA and/or the DfE. We collect and use personal data in order to meet legal requirements and legitimate interests set out in the GDPR and UK law, including those in relation to the following:

- ☐ Article 6 and Article 9 of the GDPR
- ☐ Education Act 1996
- ☐ Section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013

In accordance with the above, the personal data of pupils and their families is collected and used for the following reasons:

- ☐ To support pupil learning
- ☐ To monitor and report on pupil progress
- ☐ To provide appropriate pastoral care
- ☐ To assess the quality of our service
- ☐ To comply with the law regarding data sharing

##### Which data is collected?

The categories of pupil information that the school collects, holds and shares includes the following:

- ☐ Personal information – e.g. names, gender, date of birth, pupil numbers and addresses
- ☐ Characteristics – e.g. ethnicity, language, nationality, country of birth and free school meal eligibility
- ☐ Attendance information – e.g. number of absences and absence reasons
- ☐ Assessment information – e.g. national curriculum assessment results
- ☐ Relevant medical information
- ☐ Information relating to SEND
- ☐ Behavioural information – e.g. number of temporary exclusions
- ☐ Photographs – these will be used to aid our records management.

Whilst the majority of the personal data you provide to the school is mandatory, some is provided on a voluntary basis. When collecting data, the school will inform you whether you are required to provide this data or if your consent is needed. Where consent is required, the school will provide you with specific and explicit information with regards to the reasons the data is being collected and how the data will be used.

The categories of parent information that the school collects, holds and shares includes the following:

- ☐ Contact information, including addresses, phone numbers and email addresses of parents and/or any other emergency contacts
- ☐ Information pertaining to home life where appropriate, e.g. where a pupil is identified as having a mental health issue or there are safeguarding concerns

### **How long is your data stored for?**

Personal data relating to pupils at Hagley Primary School and their families is stored in line with the school's GDPR Data Protection Policy.

In accordance with the GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected.

### **Will my information be shared?**

The school is required to share pupils' data with the DfE on a statutory basis.

The National Pupil Database (NPD) is managed by the DfE and contains information about pupils in schools in England. Hagley Primary School is required by law to provide information about our pupils to the DfE as part of statutory data collections, such as the school census; some of this information is then stored in the NPD. The DfE may share information about our pupils from the NDP with third parties who promote the education or wellbeing of children in England by:

- ☐ Conducting research or analysis.
- ☐ Producing statistics.
- ☐ Providing information, advice or guidance.

The DfE has robust processes in place to ensure the confidentiality of any data shared from the NDP is maintained.

Hagley Primary School will not share your personal information with any third parties without your consent, unless the law allows us to do so. The school routinely shares pupils' information with:

- ☐ Pupils' destinations upon leaving the school
- ☐ The LA
- ☐ The NHS
- ☐ Our School Communication Portal
- ☐ Assessments and Provision programme

### **What are your rights?**

Parents and pupils have the following rights in relation to the processing of their personal data.

You have the right to:

- ☐ Be informed about how Hagley Primary School uses your personal data.
- ☐ Request access to the personal data that Hagley Primary School holds.
- ☐ Request that your personal data is amended if it is inaccurate or incomplete.
- ☐ Request that your personal data is erased where there is no compelling reason for its continued processing.
- ☐ Request that the processing of your data is restricted.
- ☐ Object to your personal data being processed.

Where the processing of your data is based on your consent, you have the right to withdraw this consent at any time.

If you have a concern about the way Hagley Primary School and/or the DfE is collecting or using your personal data, you can raise a concern with the ICO. The ICO can be contacted on 0303 123 1113, Monday-Friday 9am-5pm.

### **Where can you find out more information?**

If you would like to find out more information about how we and/or the DfE collect, use and store your personal data, please visit our website or the DfE's website [www.gov.uk](http://www.gov.uk).

## Appendix 2

### A blank data breach form

**Data Breach** ICO Telephone number 0303 123 1113

<b>Date reported to DPO:</b>		<b>Date Breach occurred:</b>	
<b>Date Breach investigation started:</b>		<b>Date Breach reported to ICO:</b>	
<b>What has happened?</b>			
<b>When and how you found out about the breach:</b>			
<b>The people that have been or may be affected by the breach:</b>			
<b>What you are doing as a result of the breach:</b>			
<b>Who we should contact if we need more information:</b>			
<b>Who else has been told:</b>			
<b>Reported to ICO:</b>	Yes/No	<b>Date reported:</b>	
<b>Signed:</b>		<b>Name:</b>	

## **Freedom of Information Policy**

### **1. Introduction: what a publication scheme is and why it has been developed**

One of the aims of the Freedom of Information Act 2000 (which is referred to as FOIA in the rest of this document) is that public authorities, including all maintained schools, should be clear and proactive about the information they will make public.

In order to meet this aim, we have produced a publication scheme, setting out:

- The classes of information which we publish or intend to publish;
- The manner in which the information will be published; and
- Whether the information is available free of charge or on receipt of payment.

The scheme covers information already published and information which is to be published in the future. All information in our publication scheme is available on request.

Some information which we hold may not be made public, for example personal information.

This publication scheme conforms to the model scheme for schools approved by the Information Commissioner.

### **2. Aims and Objectives**

The school aims to:

- Develop open and secure relationships which promote good communication and a shared understanding;
- Engage and challenge the whole child by developing a range of skills and abilities through a curriculum that offers a wide variety of experience;
- Develop a positive and strong work ethic to learning and encourage each individual to reach their full potential;
- Insist on high standards of behaviour and polite conduct respecting the needs of others;
- Promote individuals to take responsibility for their actions and to be aware that they are stewards of their environment;
- Provide a well-resourced and orderly learning environment where high standards of work and presentation are seen as models of excellence;
- Develop a committed school community which uses its full potential to work as a team for the common good in a supportive and positive manner.

This publication scheme is a means of showing how we are pursuing these aims.

### **3. Categories of information published**

The publication scheme guides you to information which we currently publish (or have recently published) or which we will publish in the future. This is split into categories of information known as 'classes'.

The classes of information that we undertake to make available are organised into broad topic areas:

- General information about the school, e.g. its staff, leadership and governance, information about the curriculum, school terms and events
- Information about the school's performance, e.g. Ofsted report and results of SATs Pupils & Curriculum – information about policies that relate to pupils and the school curriculum
- School Policies and other information related to the school - information about policies that relate to the school in general

A detailed guide to the information available and how to access it is attached as appendix A.

#### **4. How to request information**

If you require a paper version of any of the documents within the scheme, please contact the school by telephone, email or letter (contact details are set out below) or you can visit our website at [www.hagleyprimary.org.uk](http://www.hagleyprimary.org.uk).

Email: [office@hagleyprimary.worcs.sch.uk](mailto:office@hagleyprimary.worcs.sch.uk)

Tel: 01562 883280

Contact Address: Hagley Primary School, Park Road, Hagley, Stourbridge, DY9 0NS

To help us process your request quickly, please clearly mark any correspondence "PUBLICATION SCHEME REQUEST" (in CAPITALS please) If the information you're looking for isn't available via the scheme and isn't on our website, you can still contact the school to investigate further.

#### **5. Paying for information**

Information published on our website is free, although you may incur costs from your Internet service provider. If you don't have Internet access, you can access our website using a local library or an Internet café.

If your request means that we have to do a significant amount of photocopying, printing, pay a large postage charge, or is for a priced item such as some printed publications or videos we will inform you of any cost before fulfilling your request. Information will be charged at the actual cost of providing it (i.e. the cost of photocopying, plus time of employee photocopying information, plus postage and any other actual costs incurred as a result of providing the requested information). If we need to charge for providing the information, we will require payment before we can provide the information.

#### **6. Further information**

For further information about the Freedom of Information act and your rights, please refer to the Information Commissioner's website: <http://www.ico.gov.uk>