Hagley Primary School

GDPR Data Protection Policy

Date reviewed: **September 2021**

Date of next review: **September 2022**

Responsible member of staff: **Sarah Edwards**

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 Sarah Edwards who is contactable at Hagley Primary School, Park Road, Hagley, DY9 0NS, 01562 883280, 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 in order 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.

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. If consent is given in a document which deals with other matters, the consent from be kept separate from those other matters

  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.

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 employmentlaw 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 21 days.

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 itis no longer required in accordance with the 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 school's policies).
- 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.

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 datawas 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.

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.

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 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 Informationand 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.