Data Protection Policy (GDPR compliant)

1. Aim and scope of policy

This policy applies to the processing of personal data in manual and electronic records kept by the School. It also covers the School's response to any data breach and other rights under the General Data Protection Regulation.

This policy applies to the personal data of students, parents, carers, guardians, job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

2. Definitions

i) **Personal data** is information that relates to a person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier or pseudonym.

ii) **Special categories of personal data**" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

iii) **Criminal offence data** is data which relates to an individual's criminal convictions and offences.

iv) **Data processing** is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. This includes collection, recording, organisation, storage, adaptation or alteration, retrieval, disclosure, erasure or destruction. The lawful bases for processing are set out in Article 6 of the UK GDPR

v) **Data subject** – The identified or identifiable individual whose personal data is held or processed

vi) **Data controller** – A person or organization that determines the purpose and the means of processing personal data

vii) **Data processor** - A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

The School makes a commitment to ensuring that personal data, including special categories of personal data and criminal offence data is processed in line with GDPR and domestic laws and all its employees conduct themselves in line with this, and other related, policies. Where third parties process data on behalf of the School, the School will ensure that the third party takes measures to maintain the School's commitment to protecting data. In line with GDPR, the School understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

3. Types of Data Held

The following types of data may be held by the School, as appropriate, on relevant individuals:

- Employee and worker Personal data is kept in personnel files or within the School's HR and payroll systems including:
    - name, address, phone numbers - for individual and next of kin
    - recruitment information including application forms, references from former employers and other relevant identification information required for safeguarding and proof of the right to work in the UK
    - National Insurance numbers and tax codes
    - job title, job descriptions and pay grades
    - conduct issues such as letters of concern, disciplinary proceedings
    - Capability issues and proceedings
    - Payment claim forms including overtime and lettings payments
    - internal performance information
    - medical or health information
    - sickness and other categories of absence records
    - Payroll numbers
    - terms and conditions of employment
    - Training details.
    - Log in credentials
    - Email contact addresses
    - Timesheets/Staff Timetables

- Student data is held in personal student files and within the Schools Data Systems including:
    - name, address, phone numbers - for individual students and their parent, carer or guardians
    - sensitive data relating to students required by Department of Education including UPN, gender, ethnicity, Date of Birth
    - log in credentials for systems accessed by students eg: Epraise, renaissance learning, rising stars
    - Student timetables
    - free school meals entitlement information
    - catering data for example details of student loans
    - Photographs of students
    - conduct issues such as letters of concern, requests for holidays in term time
    - exclusion information including correspondence with Local Authority Childrens Services
    - attendance related information and records
    - safeguarding, child protection and pastoral related information relating to individual students
    - behaviour logs such as Epraise
    - learning progress information for example School Reports
    - results of KS2 tests and other relevant tests/assessments taken at Middle School
    - results of internal examinations
    - results of external examinations
    - Special educational needs information including Independent Education Plans (IEP) and Education Health Care Plans (EHCP)

    - Alternative curriculum information including Work Experience placement records

- CCTV and Biometric Data
    - CCTV footage taken of the school site
    - biometric for example identification data for catering purposes

- Medical Health Information
    - Accident forms as required for students, parents, carers, guardians, job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors
    - Risk assessments as required students, parents, carers, guardians, job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors
    - Lists of First Aiders on site
    - Care plans for students with specific medical needs
    - List of students with epipens

- Supplier, lettings and contractor information
    - Contact names, telephone, email and addresses
    - Bank details
    - Invoice, supplier statements and credit notes
    - Details of Training courses delegates and copies of certification if required for example, Qualsafe, DSE, Safeguarding
    - GDPR processor contracts
- Parents, Teachers and Friends Association contact details including names, telephone numbers, emails and addresses
- Finance Information
    - Petty cash Forms and other general receipts for money given eg school trips
    - Budget reports showing staffing salary information
    - Parent Pay information to facilitate payment of monies eg Catering and school trips

Relevant individuals should refer to the School's privacy notices and Data Retention policy for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

4. Data Protection Principles

All personal data obtained and held by the School will:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit, and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes of processing
- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay
- not be kept for longer than is necessary for its given purpose
- be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- comply with the relevant GDPR procedures for international transferring of personal data.

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure)
- the right to restrict the processing of the data
- the right to portability
- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.

5. Procedures

The School has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

- it appoints or employs employees with specific responsibilities for:
    a. the processing and controlling of data
    b. the comprehensive reviewing and auditing of its data protection systems and procedures
    c. overviewing the effectiveness and integrity of all the data that must be protected.

  There are clear lines of responsibility and accountability for these different roles.

- it provides information to relevant individuals on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way
- it provides its employees with information and training to make them aware of the importance of protecting personal data, to teach them how to do this, and to understand how to treat information confidentially
- it can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with
- it carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by the School
- it recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. The School understands that consent must be freely given, specific, informed and unambiguous. The School will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time
- it has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences

- it is aware of the implications international transfer of personal data internationally.

6. Access to data

Relevant individuals have a right to be informed whether the School processes personal data relating to them and to access the data that the School holds about them. Requests for access to this data will be dealt with under the following summary guidelines:

- a form on which to make a subject access request is available from *the schools website.* The request should be made to the **Data Protection Officer** (contact details are shown below).
- the School will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the Student/parent or carer or employee making the request
- the School will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous.

Relevant individuals must inform the School immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. The School will take immediate steps to rectify the information.

For further information on making a subject access request, Student/parent or carer or employees should refer to our subject access request policy, available from *our website (see contact details below)*

7. Data disclosures (Employees)

The School may be required to disclose certain data/information to a third party. The circumstances leading to such disclosures include:

- any employee or student benefits operated by third parties
- disabled individuals - whether any reasonable adjustments are required to assist them in school
- individuals' health data - to comply with health and safety or occupational health obligations towards the employee or students
- for Statutory Sick Pay purposes
- HR management and administration - to consider how an individual's health affects his or her ability to do their job
- the smooth operation of any employee insurance policies or pension plans.
- Census information required by the Department of Education with regard to students or employees
- Safeguarding issues relating to students
- The smooth operation of any insurance policies

These kinds of disclosures will only be made when strictly necessary for the purpose.

8. Data security

The School adopts procedures designed to maintain the security of data when it is stored and transported. More information can be found in the data transfer security policy, available *from the school website (see contact details below)*

In addition, employees must:

- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- check regularly on the accuracy of data being entered into computers
- always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them
- use computer screen blanking to ensure that personal data is not left on screen when not in use.

Personal data relating to relevant individuals should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by the Headteacher. Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary
- using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
- ensuring that laptops or USB drives are not left lying around where they can be stolen.

Failure to follow the School's rules on data security may be dealt with via the School's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

9. International data transfers

The School does not transfer personal data to any recipients outside of the EEA.

10. Breach notification

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of the School becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual.

If the breach is sufficient to warrant notification to the public, the School will do so without undue delay.

11. Training

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for the School are trained appropriately in their roles under the GDPR.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the School of any potential lapses and breaches of the School's policies and procedures.

12. Records

The School keeps records of its processing activities including the purpose for the processing and retention periods in its Data Record. These records will be kept up to date so that they reflect current processing activities.

13. 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.

14. Data Protection Officer

The School's Data Protection Officer is the *Head of Governance and Compliance* who can be contacted at Droitwich Spa High School and Sixth Form Centre, Briar Mill, Droitwich, WR9 0AA or by email at privacy@droitwichspahigh.worcs.sch.uk .

15. Chief Privacy Officer

The HR and Administration Manager is the School's appointed chief privacy officer in respect of its data protection activities who can be contacted at Droitwich Spa High School and Sixth Form Centre, Briar Mill, Droitwich, WR9 0AA or by email at privacy@droitwichspahigh.worcs.sch.uk

16. The School Website Privacy Page

The Data Protection Policy is linked to our Privacy notices and Freedom of Information Policy. The schools' policies, privacy notices and forms are available on our web site at www.droitwichspahigh.worcs.sch.uk or by using the link below

https://public.droitwichspahigh.worcs.sch.uk/privacy