WEST DERBY SCHOOL

STAFF DATA PRIVACY POLICY

This policy will be reviewed:	Annually
Last reviewed on:	22 March 2023
Approved on:	27 March 2024
Next review date:	31 March 2025
Signed:	S Graham (Headteacher)
Signed:	K Hodgkiss (On behalf of the Trust)

Introduction
This policy contains important information about how and why West Derby School collects, processes, stores and shares Personal Data belonging to our employees, workers and third parties e.g. pupils and parents (**Third Party Data**).

The focus of this policy is on the School's duties and responsibilities in respect of the Personal Data of our employees and workers (**Staff**), and the duties and responsibilities our Staff have to Process the Personal Data of our Staff and Third Party Data in accordance with our policies, procedures and the law.

This policy should be read in conjunction with our:

- GDPR and Pupil Records Policy;
- Privacy Notice for School Workforce;
- Disciplinary Policy.

And the

- Data retention guidance incorporated in the Information Management Toolkit for Schools (www.imrs.org.uk), which the school follows for retention of data.

Data Privacy: The Basics
In legal terms, this process of collecting and processing Personal Data means that the School is referred to as a Controller (**Controller**). Any external person or organisation that Processes Personal Data on our behalf and on our instructions (e.g. a payroll provider or insurance company) is referred to a Data Processor (**Processor**).

Any activity that involves the use of Personal Data is referred to as Processing (**Processing/Process/Processes**). It includes:

- Obtaining, recording or holding Personal Data;
- Carrying out any operation or set of operations on Personal Data (e.g. organising, amending, retrieving, using, disclosing, erasing or destroying it); and
- Transmitting or transferring Personal Data to third parties.

Personal Data is any information identifying or relating to an identifiable Data Subject (**Personal Data**). A person is considered to be a Data Subject if he or she is a living individual that can be identified (directly or indirectly) from the Personal Data (**Data Subject**).

Personal Data can include information relating to you that has been 'pseudonymised', meaning that any information that directly or indirectly identifies you (e.g. your name) is removed and replaced with one or more artificial identifiers or pseudonyms (e.g. an employee reference number). However, truly anonymous data, or data that has had any identifying information permanently removed from it, does not count as Personal Data. When considering whether information 'relates to' you for the purposes of Data Protection Legislation, the School takes into account a range of factors, including the content of the information, the purpose or purposes for which we are Processing it, and the likely impact or effect of that Processing on you.

Personal Data includes some Special Category Data and Criminal Offence Data. The following table gives a non-exhaustive list of examples of what is included and excluded from these definitions:

Personal Data		Excluded / Not Personal Data
Personal Data	**Special Category Personal Data (formerly called Sensitive Personal Data)**	
• Name • Address • Telephone number • Date of birth • Gender • Qualifications • Opinions about an individual's actions or behaviour (e.g. references, Staff appraisals, disciplinary records) • Location data	• Racial or ethnic origin • Political opinions • Religious or similar beliefs • Trade union membership • Physical or mental health conditions (e.g. sick notes, medical reports) • Sexual life • Sexual orientation • Gender identity • Biometric or genetic data • Sickness absence data	• Anonymous data • Data that has had the individual's identity permanently removed (e.g. statistical information about the gender breakdown of our Staff from whom individuals cannot be identified)

Most of the information the **School** Processes is provided to us directly by you for one of the following reasons:

- to enable the development of a comprehensive picture of the workforce and how it is deployed;
- to improve the management of the School's employees;
- to inform the development of recruitment and retention policies;
- to communicate with you in connection with your employment and role;
- to understand how your physical or mental health may be relevant to your work;
- to keep appropriate records required by law and/or for employment law purposes;
- to monitor your performance or conduct;
- to enable you to be paid; and,
- to enable the monitoring of selected protected characteristics.

We also receive personal information indirectly, from the following sources;

- Her Majesty's Revenue and Customs (HMRC);
- The Disclosure and Barring Service (DBS);
- Medical Professionals; and,
- Referees during the recruitment process.

Your rights as a Data Subject

Each Data Subject has legal rights designed to protect the privacy of their Personal Data. You are a Data Subject (with regard to your own Personal Data). This policy explains more about your rights as a Data Subject and your responsibilities in relation to Processing Personal Data of Third Parties.

Third Party Data: your duties and responsibilities

To the extent that you are involved in the Processing of Personal Data, you will have legal duties and responsibilities to Process the Personal Data of others in accordance with this policy and the law governing data privacy, including the UK GDPR (see "Our commitment to complying with data protection procedures" below).

Data privacy: our collective responsibility

The School takes its legal obligations and responsibilities regarding data privacy very seriously. We expect all of our Staff to treat any Personal Data they may come into contact with (whether it is part of their role to handle such data or not) sensitively and in accordance with our data privacy policies and procedures. You are reminded that any breach of this policy, our data privacy procedures, or the law governing data privacy, may result in disciplinary action.

Our Commitment to Complying With the Data Protection Principles

Personal Data must be Processed in compliance with the Data Protection Principles (DPP) relating to the Processing of Personal Data (as set out in the UK General Data Protection Regulation (UK GDPR). The DPP require Personal Data to be:

Data Protection Principle (DPP)	Details
Processed lawfully, fairly and in a transparent manner	Personal Data must be Processed on the basis of one or more of the conditions specified in the UK GDPR.
Collected only for specified, explicit and legitimate Purposes.	If we collect Personal Data directly from Data Subjects, we will inform the Data Subject about: • The Purpose(s) for which we intend to Process their Personal data; • The third parties (if any) with which we will share, or to which we will disclose, their Personal Data; and • Their rights as a Data Subject (e.g. to access and rectify their Personal Data). Personal Data must not be Processed in any manner incompatible with those original purposes.
Adequate, relevant and limited to what is necessary in relation to the Purposes for which it is Processed.	We will only collect Personal Data to the extent that it is required for the specific Purpose notified to the Data Subject.
Accurate and where necessary kept up to date	We will ensure that Personal Data we hold is accurate and kept up to date. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You are required to keep us informed of any changes to your Personal Data so that we can keep our records accurate We will take all reasonable steps to, without delay, destroy or amend inaccurate or out-of-date Personal Data.
Not kept in a form which permits identification of a Data Subject for longer than is necessary for the Purposes for which the data is Processed.	We follow current data retention guidelines and have procedures for the deletion and destruction of data in accordance with those guidelines.

Data Protection Principle (DPP)	Details
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.	We will take appropriate security measures against unlawful or unauthorised Processing of Personal Data, and against the accidental loss of, or damage to, personal data. We have put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal data will only be transferred to a Data Processor if they agree to comply with those procedures and policies, or if they also put in place adequate security measures.
Made available to the Data Subject on request and that Data Subjects are allowed to exercise certain rights in relation to their Personal Data	We will Process all Personal Data in line with Data Subjects' rights, in particular their right to: • Request access to any Personal Data held about them; • Prevent the Processing of their Personal Data for direct-marketing Purposes; • Ask to have inaccurate Personal Data amended; and • Prevent Processing that is likely to cause damage or distress to themselves or anyone else.
Not transferred to people/organisations situated in countries without adequate protection	We may only transfer any Personal Data we hold to a country outside the UK, provided that one of the following conditions applies: • The country ensures an adequate level of protection for the Data Subjects' rights and freedoms; • The Data Subject has given consent; • The transfer is necessary for one of the conditions set out in the UK GDPR (e.g. for the performance of a contract between us and the Data Subject, or to protect the vital interests of the Data Subject); • The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims; or • The transfer is authorised by the Information Commissioner where we have adduced adequate safeguards with respect to the protection of the Data Subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Conditions for Processing
To be Processed lawfully, Personal Data must be Processed on the basis of one or more of the Conditions specified in the UK GDPR (Condition(s)). The most common Conditions we rely on to Process Personal Data are:

Conditions for Processing which we commonly rely on	
Personal Data	**Special Category Personal Data** **(formerly called Sensitive Personal Data)**
• The Data Subject has given their consent to the Processing for one or more specific Purposes; • Processing is necessary for entering or performing a contract with the Data Subject; • Processing is necessary for compliance with a legal obligation to which the Controller is subject; • Processing is necessary to protect the vital interests of the Data Subject; or • Processing is necessary for the Purposes of legitimate interests pursued by the data controller or by a third party.	• The Data Subject has given explicit consent to the processing for one or more specific Purposes; • Processing is necessary for the Purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment and social security and social protection lawso far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; • Processing is necessary to protect the vital interests of the Data Subject or of another natural person, where the Data Subject is physically or legally incapable of giving consent; • Processing is necessary for the establishment, exercise or defence of legal claims; or • Processing is necessary for the Purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

However, we may in some circumstances rely on other Conditions set out in the UK GDPR or Data Protection Act 2018 to justify the Processing of Personal Data or Special Category Personal Data. The table below sets out the conditions from processing criminal offence data and the additional conditions we may rely upon if processing under applicable Article 9 conditions.

Conditions for Processing	
Criminal Offence Data	**Special Category Personal Data (DPA 2018 conditions)**
• Employment, social security and social protection • Research • Preventing or detecting unlawful acts • Preventing fraud • Suspicion of terrorist financing or money laundering • Counselling • Safeguarding of children and of individuals at risk • Insurance • Consent • Protecting individual's vital interests • Personal data in the public domain • Administration of accounts used in commission of indecency offences involving children	• Employment, social security and social protection • Research • Equality of opportunity or treatment • Racial and ethnic diversity at senior levels of organisations • Preventing or detecting unlawful acts • Preventing fraud • Suspicion of terrorist financing or money laundering • Support for individuals with a particular disability or medical condition • Counselling • Safeguarding of children and of individuals at risk • Insurance

Personal Data must only be collected or Processed for specified, explicit and legitimate Purposes. The School will establish and record the Condition for Processing each time Processing of Personal Data occurs.

Staff are forbidden from Processing Personal Data for Purposes which go beyond or are incompatible with the original Purposes specified to the Data Subject in the transparency information provided to them (see "Transparency: notifying Data Subjects" below).

Criminal Offence Data

Where appropriate and legally permitted, we collect Criminal Offence Data as part of the recruitment process (e.g. when we conduct a standard or enhanced DBS criminal record check). We may also be notified from time to time of Criminal Offence Data in the course of employment (e.g. if you are suspected to have committed a crime, or if you report a criminal conviction to us).

We will use Criminal Offence Data we hold in the following ways:

1.1 To determine whether your criminal record (i.e. the results of a standard or enhanced DBS check) impacts upon your suitability to be offered employment;

1.2 To consider whether any criminal charges, prosecutions or convictions (including cautions you accept) that occur during your employment warrant impact upon your continued suitability for your role, and/or must be reported by us to our insurers, or to regulatory authorities (e.g. the Teaching Regulation Agency)

1.3 Where it is relevant, in the context of a disciplinary or grievance process.

We will only collect and Process Criminal Conviction Data if it is appropriate given the nature of the role, and where we have a lawful basis to do so. This will usually be where Processing is necessary to carry out our obligations. We have in place an appropriate policy document and safeguards that we are required by law to maintain when Processing Criminal Conviction Data.

Processing the Personal Data of Third Parties

In some limited circumstances, and for specified purposes, we will also Process Personal Data relating to third parties, such as your next of kin and/or dependants. For example, we may need to Process their personal data for the purposes of administering any insurance and pension survivor benefits they may be entitled to. Where this occurs, we may contact your next of kin and/or dependants separately to explain why we need to Process their Personal Data.

Consent

Consent (Consent) is one of the many Conditions upon which the Processing of Personal Data can be based. However, in lots of circumstances the School will rely on other Conditions to process Personal Data. For example, the School does not routinely rely on Consent as a Condition to justify the Processing the Personal Data of our Staff. This is explained further in your personal Privacy Notice for School Workforce.

Key points to note about relying on Consent as a Condition for Processing:

- Consent requires affirmative action; silence, pre-ticked boxes or inactivity should not be considered to be consent;
- Consent must be kept separate from other terms and conditions, so that it is clear and unambiguous;
- Use clear and plain language when explaining consent;
- Consent must be specific and informed, meaning it should be clear to the Data Subject what it is they are consenting to and how and why their Personal Data will be Processed;
- The Data Subject must be free to refuse to give their Consent to the Processing;
- If Consent is relied upon, the Data Subject must be easily able to withdraw their Consent to Processing at any time and withdrawal must be promptly honoured;
- Consent should be refreshed if Personal Data will be Processed for a different and incompatible Purpose to that disclosed when the Data Subject first consented;
- Consent should not be relied upon as a Condition for Processing where there is an imbalance of power between the School and the Data Subject; and
- Records should be kept of any Consent received (what consent was given, when and how it was obtained).

What Rights Do Data Subjects Have?

Data Subjects have rights when it comes to how we handle their Personal Data. Some of these rights are dependent on the nature and purposes of the processing. In summary, these include rights to:

- Withdraw consent to Processing at any time where we have relied on consent to conduct the Processing (see above “Consent”);
- Receive certain information about our Processing activities (see “Transparency: notifying Data Subjects” below);

- Request access to the Personal Data that we hold on them (see “Subject Access Requests” below);
- Prevent our use of their Personal Data for direct marketing purposes;
- Ask us to erase Personal Data if it is no longer necessary in relation to the Purposes for which it was collected or Processed, or to rectify inaccurate data or to complete incomplete data;
- Restrict Processing in specific circumstances;
- Challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- Prevent Processing that is likely to cause damage or distress to them or anyone else;
- Be notified of any Personal Data Breach which is likely to result in a high risk to their rights and freedoms;
- Make a complaint to the Information Commissioner; and
- In limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

Staff who wish to exercise a right on their own behalf or who receive a written request from a Data Subject who wishes to exercise any of their UK GDPR or data privacy rights (for example, requesting the rectification or deletion of their Personal Data) should contact our Data Protection Officer, Tony Card, immediately.

Data Subjects are not required to pay any charge for exercising their rights. If a request is made we must respond within one month.

Subject Access Requests

Data Subjects may make a formal written request for details of the Personal Data we hold about them (**Subject Access Request**). The UK GDPR requires us to deal with Subject Access Requests within strict time-limits which is, normally, one month form the date of receipt. Therefore, Staff who receive a written request for access to Personal Data (whether or not the request specifies that it is a Subject Access Request) should forward it to our Data Protection Officer immediately.

When receiving telephone enquiries, we will only disclose Personal Data we hold on our systems if we check the caller's identity to make sure that information is only given to a person who is entitled to it. If we are not sure about the caller’s identity, or if their identity cannot be checked, we will ask that the caller put their request in writing.

Transparency: Notifying Data Subjects

The UK GDPR requires Controllers to provide clear, detailed and specific information to Data Subjects about the Processing of the Personal Data. Such information must be provided through appropriate privacy notices. Our Privacy Notice for School Workforce sets out the information about how we Process your Personal Data. It will be reviewed annually to ensure we are as transparent as possible about the Personal Data we Process.

The UK GDPR (and the accompanying guidance) is very specific about the language used in any privacy notices. To ensure compliance with the UK GDPR the Data Protection Officer must be involved in the drafting of any privacy notices.

Purpose Limitation
Personal Data must be collected only for specified, explicit and legitimate Purposes (Purposes) and must not be further Processed in any manner incompatible with those Purposes. This means that we cannot use Personal Data for new, different or incompatible Purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new Purposes, and (if this is the Condition relied upon to Process their Personal Data) they have given their Consent. To ensure compliance with this Purpose limitation requirement:

- The School will establish and record the Purposes for Processing each time Personal Data is collected;
- Staff who are responsible for collecting or Processing Personal Data must ensure on each occasion that the Purposes for doing so are not incompatible than the original specified Purposes. If the Purposes are incompatible, the Data Subject must be notified of the new Purposes as soon as possible.

You are reminded that Processing Personal Data for Purposes which are incompatible with the Purposes for which the Personal Data was obtained is considered a serious breach of this policy and may result in disciplinary action.

Data Minimisation
Personal Data must be adequate, relevant and limited to what is necessary in relation to the Purposes for which it is Processed. This means that you:

- May only collect or Process Personal Data when performing your job duties requires it;
- Cannot Process Personal Data for any reason unrelated to your job duties;
- Must not collect excessive Personal Data, which is not relevant for the specified Purposes;
- Must ensure that when any Personal Data is no longer needed for the specified Purposes, it is deleted or anonymised in accordance with the Information Management Toolkit for Schools (www.imrs.org.uk), which the school follows for retention of data.

Data Accuracy
Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. To the extent that your job requires you to collect or Process Personal Data, this means that you:

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

Storage Limitation
Personal Data must not be kept in an identifiable form for longer than is necessary for the Purposes for which the data is Processed. The School (and to the extent that your duties involve the Processing of Personal Data, you) must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate Purposes for which we originally collected it.

The Schools' Information Management Toolkit for Schools (www.imrs.org.uk), which the school follows for Data Retention is designed to ensure Personal Data is deleted after a reasonable time, unless a law requires such Personal Data to be kept for a minimum time. This guidance is available in hard copy format upon request.

The School (and to the extent that your duties involve the Processing of Personal Data, you) will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with the IMRS guidance for Data Retention.

Data Security

The School will take appropriate security measures against unlawful or unauthorised Processing of Personal Data, and against the accidental loss of, or damage to, Personal Data. We have procedures and technologies in place which are designed to maintain the security of Personal Data from the point of collection to the point of destruction. In summary, this means that the School and our Staff must ensure that:

- Only people who are authorised to use the Personal Data can access it;
- Steps are taken to ensure that people who are authorised to access Personal Data are not accessing or Processing Personal Data for reasons which are unrelated to their job role;
- Steps are taken to verify the identity of a Data Subject before discussing their Personal Data with them;
- Personal Data is stored on the School's central computer system instead of individual PCs, laptops, tablet devices, mobile telephones etc;
- Computers and laptops are not left unattended without locking their screens via password controls to prevent unauthorised access;
- Personal Data is not carried off-site, except when it is legally necessary to do so. Where Personal Data needs to be carried off-site in paper form, for example a set of pupils' books for marking, staff must take extreme care. Keep physical documents in a secure, closed folder along with your contact details in case the folder is lost. Store the documents in a safe place at home – don't leave them in your car or at a friend's house.
- Personal Data Breaches, or circumstances which might reasonably lead to a Personal Data Breach, are promptly reported to the Data Protection Officer (DPO) and the Director of Governance and Compliance (DGC). School has 72 hours to report any significant breaches to the ICO and it is therefore imperative that the DPO and DGC are notified as soon as a breach or suspected breach comes to light; and
- Our security procedures e.g. door entry controls, use of secure locking cupboards, shredders, use of sealed confidential waste disposal bags, password protection and secure electronic platform (Egress) for necessary document sharing are followed.

You are reminded that any breach of our data security procedures is considered a serious breach of this policy and may result in disciplinary action.

Biometric data

We use cashless payment in our catering services. Staff are entitled to use our catering offer and to make payments through the cashless system. The system uses finger scans to identify staff and to ensure the correct deduction is assigned to the member of staff's credit account.

We rely on your explicit consent to use your finger scan as part of our cashless system. It is only ever processed for this purpose and you may withdraw your consent at any time. Please contact our Data Protection Officer if you have more queries about the use of your biometric data.

Staff Training
As part of our commitment to data security, all Staff whose role involves regular Processing of Personal Data, will receive training on our data privacy policies and procedures as part of their induction and this will be refreshed at regular intervals thereafter.

Mandatory Data Breach Reporting
Under the UK GDPR the School has certain obligation to mandatorily report Personal Data Breaches. A Personal Data Breach (**Personal Data Breach**) is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

There are two levels of mandatory reporting obligation, which depend upon the level of risk arising from the Personal Data Breach:

Mandatory Reporting Obligation	**Details**
Report to Information Commissioner must be made ASAP (at latest within 72 hours of becoming aware of the Personal Data Breach).	If the Personal Data Breach is likely to result in **a risk** to Data Subject's rights and freedoms. Examples: • Report: – e-mailing details of an SEN pupil's assessments to the wrong external e-mail address; – a ransomware attack which results in all personal data being encrypted and no back-ups are available; • Do not report: – loss of a staff telephone list; – loss of a securely encrypted mobile device, provided the encryption key remains within our secure possession and this is not the sole copy of the Personal Data.
Notify Data Subject "without undue delay" and "as soon as reasonably feasible".	If a Personal Data Breach poses a **high risk** to a Data Subject then it must be directly reported to them as well as the Information Commissioner unless an exception applies. High risk situations are likely to include the potential of people suffering significant detrimental effect – for example, discrimination, damage to reputation or financial loss. Examples of high risk Personal Data Breaches: • A cyber-attack leads to Personal Data being exfiltrated from our server; • We suffer a ransomware attack which results in all Personal Data being encrypted. No back-ups are available and the data cannot be restored. There are some limited exceptions to the mandatory

Mandatory Reporting Obligation	Details
	requirement to report a Personal Data Breach to the Data Subject.

Failure to make the relevant mandatory Personal Data Breach report may lead to a financial sanction against the School.

It is the responsibility of all Staff to **immediately** report any Personal Data Breach which comes to their attention (whether it involves you or any other member of Staff, whether subordinate or senior to you), or circumstances which might reasonably be interpreted as a Personal Data Breach, or which could lead to a Personal Data Breach to the Data Protection Officer.

Data Protection Officer

The School has appointed a Data Protection Officer for GDPR purposes, who has overall responsibility for the School's policies and procedures relating to data privacy. The Data Protection Officer should be your first point of contact in the following situations:

- If you have any concerns, or require clarification, about your or the School's obligations regarding data privacy;
- If you have any feedback or suggestions about how the School can improve its data privacy and/or data security procedures;
- If you receive a request from a Data Subject seeking to:
  - Access their Personal Data (see "Subject Access Requests" above); or
  - Exercise any of their other rights as a Data Subject (see "What rights do Data Subjects have?" above), such as to withdraw their Consent to Processing;
- If you become aware of any member of Staff:
  - Abusing their role to access Personal Data for non-permitted reasons;
  - Processing Personal Data in a manner which is inconsistent with this policy;
  - Committing a breach of our retention guidelines.
- If you, or any other member of Staff (whether subordinate or senior to you), are involved in a Personal Data Breach, or circumstances which might reasonably be interpreted as a Personal Data Breach, or which could lead to a Personal Data Breach (see "Mandatory Data Breach Reporting" above).

Our Data Protection Officer is: Tony Card

His contact details are: Telephone- 0151 235 1315; Email- a.card@westderbyschool.co.uk ; Postal address – West Derby School, 364 West Derby Road, L13 7HQ