# West Monmouth School

# Data Protection Policy

Date Approved by Governors: May 2023

## DOCUMENT CONTROL

| | | | |
|---|---|---|---|
| **Title:** | **Data Protection Policy** | | |
| **Document Owner:** | **Headteacher** | | |
| **Document Author:** | | | |
| **Reference:** | **SCHOOL IG001** | **Retention Period:** | **Until next review** |
| **Document Classification:** | Official | **Location:** | |
| **Version / Status:** | Live | **Approved by:** | May 2023<br>PSJCC<br>SCHOOL /BOARD GOVERNORS |
| **Current Issue Date:** | May 2023 | **Next Review Date:** | May 2026 |

## REVISION HISTORY

| Issue Date | Version / Status | Reason for Change | Changed By: |
|---|---|---|---|
| Jan 2019 | 1.0 Live | Policy Implementation | A Price |
| Dec 2019 | 2.0 Live | Policy refresh following audit | A Price |
| April 2021 | 2.0 Live | Change to UK GDPR | A Price |
| Jan 2023 | 3.0 Draft | Full 3-year policy review | A Price |

## Table of Contents

# 1. PURPOSE

West Monmouth School is committed to full compliance with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 and is registered with the Information Commissioners Office as a data controller. To achieve this commitment, information about our employees and other clients and contacts must be collected and used fairly, stored safely and not unlawfully disclosed to any other person. These may include current, past and prospective employees, clients, customers, suppliers, volunteers and visitors. In addition, we may be required by law to collect and use information to comply with the requirements of central government.

# 2. SCOPE

This policy and legislation apply to all personal information held and processed by the School or held and processed on behalf of the School. This includes information held in file systems, on paper and in electronic formats, inclusive of CCTV and voice recordings.

This policy applies to: Governors, employees, whether office based or working via remote access, including contractors, volunteers, agencies and partner organisations operating on behalf of the School.

# 3. AIMS AND OBJECTIVES

All staff should be aware that information will only be processed in compliance with laws on privacy and data protection. Specifically that the principles under Chapter 2 Article 5 of the UK GDPR personal information must be:

- Processed lawfully, fairly and in a transparent manner
- Must be collected for specified, explicit and legitimate purposes
- Personal data must be adequate, relevant and not excessive
- Personal data must be accurate and kept up to date
- Personal data must be kept for no longer than is necessary
- Must be processed in a secure manner

Once personal information has been collected, we must have a lawful basis to process this data as set out in Article 6 of the UK GDPR. At least one of these must apply whenever we process personal data:

**(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

**(b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

**(c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

**(d) Vital interests:** the processing is necessary to protect someone's life.

**(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

**(f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Data subjects have defined rights over the use of their data . These rights have been reinforced and extended by the Data Protection Act 2018 and Chapter 3 Articles 13 – 22 of the UK GDPR. They apply to all, including children, however a request received from a child should be reviewed on a case-by-case basis. See info at Annex 1.

These rights are:

- The right to be informed Art 13 and 14
- The right of access Art 15
- The right to rectification Art 16
- The right of erasure Art 17
- The right to restrict processing Art 18
- The right to data portability Art 20
- The right to object Art 21
- Rights in relation to automated decision making and profiling. Art 22

The School will ensure that individuals are made aware of personal information being held by the school and how this information is being used, held, who can access it, with whom it is being shared and for how long it will be kept by providing a general Privacy Notice which is displayed on the schools website. Please note that there are instances, as permitted by the UK GDPR when individuals will not be made aware of this information, e.g. in connection with the prevention and detection of crime. The school also maintain a record of processing activities outlining what personal data is being processed by the school.

## 4. RESPONSIBILITIES

Maintaining the security, confidentiality, integrity and availability of all School information, is the responsibility of all those employed or contracted to undertake work on behalf of the School.

| | |
|---|---|
| Head teacher and Governors | Overall executive responsibility for the policy and standards and their application throughout the School |

| | |
|---|---|
| Data Protection and Information Governance Team | Policy formulation and review and providing advice and guidance<br>Ensuring that the policy (and any related procedures and standards) are kept up to date and relevant to the needs and obligations of the School |
| Head teacher | The Head teacher will be advised of all data protection events and incidents and in liaison with the Data Protection and Information Governance Team undertake, asses monitor and action information security protocols, data security breaches and incidents and assist in reporting to the Information Commissioner's Office if required.<br><br>The School is registered as a data controller with the Information Commissioners Office (ICO) and the Head teacher will renew this registration annually. |
| Head teacher/Senior Management Team/Bursar | Ensure the provision of data protection training for staff within the School.<br><br>Development of best practice guidelines.<br><br>Undertaking compliance checks to ensure adherence throughout the school with UK GDPR and the Data Protection Act 2018.<br><br>Ensure all staff are aware of how to deal with and respond to a security breach and a Subject Access Request and Education Record Request. See Appen 1<br><br>To provide a record of processing activities which must be kept up to date. More information can be found at the ICO website www.ICO.gov.uk<br>Ensuring that Policies & Procedural documents are made known to all staff, inclusive of agency workers, contractors, volunteers, students or anyone accessing the Council's systems or information and in doing so ensuring awareness of their responsibilities around handling personal and sensitive information. |
| All staff | To read and adhere to the Policy and related procedures/guidance when managing, storing and securely disposing of the information they create and receive during |

| | |
|---|---|
| | the course of their duties. See also Retention Policy and Secure Destruction Policy.<br>Should take reasonable steps to ensure that personal data provided to the school is accurate and kept up to date.<br>All staff are aware of how to respond to or request personal information via a Subject Access Request. See Appen 1.<br>That all staff are aware of the legal rights of the data subject including children aged under 13 and aged over 13. See Appen 1.<br>All staff are aware of how to respond to an education record request. See Appen 1<br>To report immediately any observed or suspected incidents or breaches where information has or may have been insecurely disposed of or accidently lost. Procedures can be found in the Information Data Loss policy.<br>All staff are responsible for securing personal data they use in their job, keep passwords safe and adhere to a clear desk policy when offices are unattended.<br>All staff are responsible for ensuring that media devices are securely destroyed when no longer required in line with the Schools Secure Destruction Policy.<br>All staff are responsible for the storage and secure destruction of information data in line with the Schools Retention Policy and Secure Destruction Policy.<br>All staff are responsible for ensuring that sufficient measures are put in place when sending personal/special category (personal/ sensitive) data. See Appen 1<br>All staff are aware of the rights of the individual under UK GDPR regulations these are:<br>The right to be informed<br>The right of access<br>The right to rectification<br>The right of erasure<br>The right to restrict processing<br>The right to data portability |

| | |
|---|---|
| | The right to object<br>Rights in relation to automated decision making and profiling.<br>Please see Appendix 1 regarding children under and over the age of 13.<br>To undertake any training/awareness provided |
| Shared Resource Service (SRS) | Managing the network infrastructure, ensuring system continuity and security |

## 5. LEGISLATION & KEY REFERENCE DOCUMENTS

**(Please note this list is not exhaustive)**

The School will abide by all relevant UK and EU legislation and the following policies and procedures:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act (2018)
- The Copyright, Designs and patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Health & Social Care Act 2001
- Social Services & Wellbeing Act 2014
- Children Act 2004
- Equality Act 2010
- Crime and Disorder Act 1998

**SCHOOL POLICIES**

- Retention Policy School-IG001
- Information Secure Destruction Policy School-IG008
- Information/Data Loss Policy School-IG003
- Request for Information Policy School-IG004
- Information Security Policy School-IG009

**SCHOOL PROCEDURES**

- Requests for Information Procedures School-IG005
- Subject Access Procedures School-IG005a
- ICT Guidance document

## 6. MONITORING AND REVIEW

The Head Teacher together with the board of governors will monitor the implementation of this policy.

This policy will be subject to review when any of the following conditions are met:

- Content errors or omissions are highlighted.
- Where another standard/guidance issued conflicts with the information in this policy.
- There will be an initial 1 year review from policy implementation.
- Thereafter reviews will be scheduled on a 3 year basis from the date of approval of the current version.

## 7. COMPLIANCE

Failure to comply with this Policy could result in disciplinary action. This could result in termination of employment and in serious cases individuals being prosecuted under the UK General Data Protection Regulation.

The school is its own Data Controller and is registered with the ICO. If you would like to exercise any of the GDPR rights outlined in this policy or make a complaint in relation to how your data has been handled you should contact:

The Head teacher

Emma.jordan@wms.schoolsedu.org.uk

If you are not satisfied you may also contact the Data Protection and Information Governance Office of Torfaen County Borough Council DPA@torfaen.gov.uk.

You may also contact the Information Commissioner (ICO). The Information Commissioner's Office (Wales) can be contacted at: The Information Commissioner's Office (Wales), 2nd Floor, Churchill House, Churchill Way, Cardiff, CF10 2HH. Telephone 0330 414 6421 e-mail Wales@ico.org.uk

## APPENDIX 1 – Key Definitions

**Data** – is defined under the Data Protection Act as:

- Information that is processed automatically
- Information that is recorded with the intention that it should be processed automatically
- Information that is recorded as part of a relevant filing system or with the intention of being part of such a system.

- Information that does not fall within the above three categories but which forms part of an accessible record. Records considered to be accessible are health records, educational records (local education authority and special schools only), local housing records and local authority social service records.
- Information which is recorded and held by a public authority which does not fall within the above 4 categories.

**Personal Data** – is data which relates to a living individual who can be identified directly or indirectly from the data. Personal data can be factual (such as name, address or date of birth, email and phone number, a Unique Pupil Reference number or an NHS number) or it can be an opinion (such as a performance appraisal ).

**Special Category Data** – is given special protections because misuse could create more significant risks to a person's fundamental rights and freedoms by putting them at risk of unlawful discrimination.

Special category date includes:

Personal data revealing racial or ethnic origin

Personal data revealing political opinions

Personal data revealing religious or philosophical beliefs

Personal data revealing trade union membership

Genetic data

Biometrics (where used for ID purposes)

Data concerning health

Data concerning a person's sex life

Data concerning a person's sexual orientation

**Personal data about criminal allegations, proceedings or convictions is not special category data**. However, there are similar rules and safeguards for processing this type of data, to deal with the particular risks associated with it.

**Data Processing** – relates to almost any activity carried out in relation to personal information. Examples are collecting, holding, processing, releasing, amending and destroying information.

**Data Controller** – an individual or organisation that decides how , why and the manner in which any personal data is processed

**Data Processor** – an individual or organisation that process personal information on behalf of the Data Controller, under instruction from the Data Controller.

**Natural Person (Data Subject)** – an individual who is the subject of the personal information.

**Personal Data Breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, disclosure of or access to personal data. A data breach which could result in a high risk to the individual must be reported to the ICO within 72 hours.

**Subject Access Request** – individuals have the right to obtain a copy of their personal data. It could be requested verbally but ideally in writing. You should act on this within one month of receipt and in most cases cannot charge a fee, however, where the request is manifestly unfounded or excessive you may charge a "reasonable fee" to comply with the request. All records that contain the personal data of the subject will be made available, subject to certain exemptions. For information on exemptions contact the DP officer. This information can then be provided in a commonly used electronic format unless the individual requests otherwise. Further information can be found in Request for Information Procedures.

**Children below the age of 13** are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our schools may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis. From the age of 13 children have a right to access their data, however each case will be assessed to determine if the child is mature enough to show understanding of what they are requesting.

**Education Record** - If a child attends a maintained school, the parent will have a right to access the child's educational record. These are records processed by or on behalf of the governing body of the school and have originated from the parent, the school or individuals engaged by or under contract to the school. An education record consists of a pupils academic achievements, skills and abilities, and progress in school including attendance, behaviour, general well being and Head teacher reports and should be answered within 15 school days.

**Sending personal sensitive data**: Information between school and Torfaen County Borough Council are encrypted to TLS1.2 (Transport layer security) and above and is secure. Information that is passed to other councils or organisations or individuals can be checked by using the email address checker as outlined below:

Check the email address is TLS 1.2 or above by using this email address checker Check TLS Website and selecting the 'Show Your SSL Version' box
If you still have concerns, contact security@srswales.com to verify the email address is accredited as being secure
If they are not accredited, you will need to:
- use the OneDrive facility, ensuring you protect the data by following the ICT Guidance document

**OR**

- password protect attachments ensuring no personal information is included within the body of the email

Generally, email addresses ending gov.uk/pnn.uk/wales.nhs.uk are secure however you must be cautious as these can be 'spoofed' and you should hover over the address to reveal the true sender before replying.