



Ysgol Gynradd Griffithstown Primary School

Data Protection Policy

Version 1.0 Draft

DOCUMENT CONTROL

Title:	Data Protection Policy		
Document Owner:	HEADTEACHER		
Document Author:	N Blackburn		
Reference:	SCHOOL-IG001	Retention Period:	Until next review
Document Classification:	Official	Location:	Griffithstown Primary School
Version / Status:	Final	Approved by:	Governors on 18.11.19
Current Issue Date:	November 2019	Next Review Date:	November 2020

REVISION HISTORY

Issue Date	Version / Status	Reason for Change	Changed By:
Jan 2018	1.0 Live	Policy Implementation	A Price
Nov 2019	2.0 Live	Policy Refresh after Audit	A Price

FILE LOCATION

Table of Contents

DOCUMENT CONTROL..... 2

REVISION HISTORY..... 2

1. PURPOSE..... 4

2. SCOPE..... 4

3. PRINCIPLES..... **Error! Bookmark not defined.**

4. OBJECTIVES 4

5. RESPONSIBILITIES 5

6. LEGISLATION & KEY REFERENCE DOCUMENTS..... 6

7. MONITORING AND REVIEW 7

8. COMPLIANCE..... 7

APPENDIX 1 – Key Definitions 8

1. PURPOSE

Griffithstown Primary is committed to full compliance with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and Data Protection Act 2018. 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. In order to operate efficiently, the School has to collect and use information about people with whom it works. These may include current past and prospective employees, clients, customers, suppliers and volunteers. In addition we may be required by law to collect and use information in order to comply with the requirements of central government.

2. SCOPE

The policy applies to all personal information held and processed by the School or held and processed on behalf of the School. This includes information 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. PRINCIPLES

The school process personal data in accordance with the six principles of GDPR and will at all times comply with its duties under Data Protection Laws.

The principles are that information should 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

4. OBJECTIVES

The Council is committed to:

- Complying with both the law and good practice
- Respecting individual's rights as defined in Chapter 11 of the GDPR 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

FILE LOCATION

- Being open and honest with individuals whose data is held
- Providing GDPR compliant documents such as: privacy notices. 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. There is a general Privacy Notice displayed on the schools website.
- Conforms to any legal and statutory requirements relating to record keeping

5. 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.

Governors and Head teacher:

Are responsible for the oversight and implementation of this policy.

Head teacher/ Senior Management Team/ School Support Staff:

It will be the responsibility of those above to ensure compliance with the policy and for communicating the policy and procedures around handling personal and sensitive information to all staff.

They will have overall responsibility for:

- The provision of data protection training for staff within the School.
- Development of best practice guidelines.
- Undertaking compliance checks to ensure adherence throughout the school with GDPR and the Data Protection Act 2018.
- Assess monitor and action information security protocols, data security breaches and incidents.
- Ensure all staff are aware of how to deal with and respond to a security breach and a Subject Access Request.
- Ensure the school is registered annually with the Information Commissioners Office (ICO)

All Staff

All staff are responsible for ensuring that any personal data which they hold is kept securely and personal information is not disclosed in any way to any unauthorised third party.

All staff are responsible for ensuring that all personal data provided to the school is accurate and up to date.

All staff are aware of how to respond to or request personal information via a Subject Access Request. That this is free unless requests are unfounded or excessive or repetitive in character. In these cases a reasonable cost is to be charged. This 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.

All staff are aware of how to respond to an education request. If a child attends a maintained school, they or their parents have a right to access an educational record. This covers information that comes from a teacher or other employee of a local authority or school, the pupil or you as a parent, and is processed by or for the school's governing body or teacher, except for information the teacher has solely for their own use. The cost depends on the number of pages provided. For example, 1 to 19 pages will cost £1.20; 20 pages will cost £2, and so on, up to a maximum of 500+ pages which will cost £50. If the request is for other information excluding the educational record then the maximum charge is £10

All staff are responsible for ensuring that incidents and breaches are reported immediately to the Head teacher. Procedures can be found in the Information Data Loss policy.

All staff are responsible for ensuring that processes outlined within the Schools Data Protection Policy & Procedures are followed at all times.

All staff are responsible for ensuring that media devices are securely destroyed when no longer required in line with the Schools Secure Destruction Policy.

All staff are responsible for the storage and secure destruction of information data in line with the Schools Retention Policy and Secure Destruction Policy.

All staff are responsible for ensuring that sufficient measures are put in place when sending personal/special category (personal sensitive) data externally. That information is encrypted, password protected or sent via Egress.

That all staff are aware of the legal rights of the data subject including children aged under 13 and aged over 13.

Contractors, Consultants and Other Parties

All contractors, consultants, partners or agents of the School must ensure that they, and all of their staff who have access to personal data held or processed for or on behalf of the School are aware of their duties and responsibilities under the GDPR.

6. 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 General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)
- 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
- Information/Data Loss Policy
- Request for Information Policy
- Information Security Policy

SCHOOL PROCEDURES

- Information/Data Loss Procedures
- Requests for Information Procedures
- Request for Information Procedures

7. 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.

8. COMPLIANCE

Failure to comply with this Policy could result in disciplinary action resulting in termination of employment and in serious cases individuals being prosecuted under the Data Protection Act /General Data Protection Regulations.

The school is its own Data Controller and if you would like to exercise any of the GDPR rights you should contact:

The Head teacher: Griffithstown Primary, Florence Place, Griffithstown, Pontypool NP4 5DN

You may also contact the Information Commissioner (ICO), however, the ICO (Wales) cannot make a decision unless you have exhausted the

FILE LOCATION

complaints/internal review procedure offered by the Council. Please do not hesitate to contact, The Head teacher: Griffithstown Primary, Florence Place, Griffithstown, Pontypool NP4 5DN or Data Protection & Information Governance Officer, Torfaen County Borough Council, Civic Centre, Pontypool, NP4 6YB. 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 any information which relates to an identified, or identifiable, living individual.

Special Category Data (Sensitive Personal) – is information relating to a living individual's race/ethnic origin, religious belief, sexual life, health – mental and physical, biometrics – where used for identification, trade union membership, political opinions or criminal/alleged criminal offences.

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 and why personal information will be 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.

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.

Education Record - If a child attends a maintained school, you or your child have a right to access your child's educational record. This covers information that comes from a teacher or other employee of a local authority or school, the pupil or you as a parent, and is processed by or for the school's governing body or teacher, except for information the teacher has solely for their own use.