



Heronbridge School

Policy: For Data Protection

Coordinator : J Evans, H Liles

Data Protection Officer:
Mr Jeremy Evans

As a Rights Respecting School, we are committed to embedding the principles of the United Nations Convention of the Rights of the Child (UNCRC). This policy enables our pupils to access and enjoy the following articles of the convention.

Article 1- Every child under the age of 18 has all the rights in the convention

Article 2 -All children have these rights

Article 19- I have the right to be protected from being hurt or badly treated

Article 28- Every child has the right to an education.

Article 42- Every child has the right to know their rights

Introduction

General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It applies to all personal information, regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically. This policy should be used in conjunction with the school's Child Protection Policy and the Digital Safety Policy

Scope of the Policy

The school as the Data Controller will comply with its obligations under the GDPR and DPA. The school is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation. All staff must have a general understanding of the law and how it may affect their decisions to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this 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 information includes factors specific to any living individual. Under the GDPR personal information also includes an identifier such as a name, an identification number or location data.

The Principles

The principles set out in the GDPR 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 it was not intended for
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to its purpose(s)
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary (Data Retention Schedule; Appendix 1)
6. Appropriate measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in an appropriate and lawful manner that ensures appropriate security of the data

Lawful Basis for processing personal information

Before any processing occurs, the purpose(s) for the processing should be made clear. Information on the lawful basis of processing personal information can be found in the school's Data Asset Register. Data subjects have the right to request withdrawal of personal information, to change consent or request access to the data we hold at any time. (Privacy notice; Appendix 2&3)

Privacy Notices

The school issues privacy notices as required, informing data subjects 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 employment purposes, the data subject shall be given all the information required by the GDPR, how and why the School will use, process, disclose, protect and retain that personal data through a privacy notice.

The School will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The School will issue a minimum of two privacy notices, one for pupil information (Appendix 2), and one for workforce information (Appendix 3), and these will be reviewed in line with any statutory or contractual changes.

The School maintains a Retention Schedule to 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 it is no longer required in accordance with the Schedule. This includes requiring third parties to delete such data where applicable.

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 person. Sensitive personal information will only be processed if there is a lawful basis for doing so, under the statutory obligations of the school.

Data Auditing

All data controllers are required to audit all personal data. This includes:

- What is it?
- Why do we need it?
- Who controls and has access to it?
- Who do we share it with?
- How long will we keep it?
- How will we keep it secure and manage risks

All of this information is held on the school's Data Eco System and data asset register.

Documentation and records

Written records of processing activities must be kept and recorded 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 personal data
- details of transfers to third parties, including documentation of the transfer mechanism safeguards in place
- retention schedule
- a description of technical and organisational security measures.

As part of the School's record of processing activities the DPO will document, or link to documentation on:

- information required for privacy notices
- records of consent
- controller-processor contracts
- the location of personal information;
- Records of data breaches.

Records of processing of sensitive information are kept on:

- The relevant purposes for which the processing takes place.
- The lawful basis for our processing
- Whether the personal information is retained or erased in accordance with the Retention Schedule and, if not, the reasons for not following the policy.

The School should conduct regular reviews of the personal information it processes and update its documentation accordingly.

Information Security

The school uses appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These measures are stated in the 'Digital Safety' policy, which should be read in conjunction with this policy. The school categorises the data according to sensitivity using a traffic system (see appendix 4).

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction.

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. Contracts with Third Party organisations must be in place.

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.

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 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 their Head teacher immediately that a data breach is discovered and make all reasonable efforts to recover the information, following the school's agreed breach reporting process.

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.

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.



Appendix 1: Retention Policy

Pupil

	Statutory Provision	Retention Period	Action at end of the administrative life of the record
Attendance		Date of register + 3 years	DESTROY
Pupil Records <ul style="list-style-type: none"> • SEN statements • Annual reviews • Annual reports • CIN reviews • Child Protection files • LAC reviews • Home/School correspondence relating to incident/injury • Tribunal information 	SEN and Disability Act	Leaving Date + 35 years (54 th Birthday)	DESTROY & DELETE OFF SYSTEM
Individual Educational Aims		Leaving Date + 35 years	DESTROY & DELETE OFF SYSTEM
Home/school correspondence		End of academic year unless relating to incident/injury	DESTROY
Correspondence about authorised absence		Date of absence +2 years	DELETE OFF SYSTEM
Permission slips where a major incident on trip		25 years for every pupil on trip	DESTROY
External Exam results		6 years	
Internal Exam results Instep sheets Accreditation units		Leaving Date + 5 years Leaving date + 1 year	DELETE OFF SYSTEM DESTROY
Informal Assessment		Current year +1 year	DESTROY
Behavior <ul style="list-style-type: none"> - PSP - Risk Matrix - Incident report slips - Risk Assessments 		25 th Birthday	DESTROY & DELETE OFF SYSTEM

- Exclusions			
Cause for concern reports		6 years after date of leaving	DESTROY & DELETE OFF SYSTEM
Manual Handling & Feeding Plans		25th Birthday	DESTROY & DELETE OFF SYSTEM
Feeding Records		Current Year + 1	DESTROY
Accident sheets		25 th Birthday	DESTROY & DELETE OFF SYSTEM



Governors

	Statutory Provision	Retention Period	Action at end of the administrative life of the record
Minutes – Principal set (signed)		Permanent	
Agendas		Until date of meeting	DESTROY
Reports		Date of report + 6 years	DESTROY & DELETE.
Instruments of Government - constitution		Retain in school whilst school is open	DESTROY
Action Plans		Date of action plan + 3 years	Destroy
Policy documents		Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process)	DESTROY & DELETE.
Complaints files		Date of resolution of complaint + 6 years.	DESTROY
Reports required by the Welsh Government		Date of report + 10 years	DESTROY & DELETE.



Management

	Statutory Provision	Retention Period	Action at end of the administrative life of the record
Correspondence created by: <ul style="list-style-type: none">• Headteacher• Deputy Headteacher• Assistant Headteacher• Heads of Department		Date of correspondence + 3 years	DESTROY
Professional development plans		6 years	
School development plans		6 years	Review
Minutes of Management Meeting		6 years	



Curriculum

	Statutory Provision	Retention Period	Action at end of the administrative life of the record
Curriculum returns		Current year + 3 years	DESTROY & DELETE
School schemes of work		Retain for as long as applicable for curriculum	DESTROY & DELETE
Timetables		Current year + 1 year	DESTROY & DELETE



Personnel

	Statutory Provision	Retention Period	Action at end of the administrative life of the record
Staff Personal Files		Termination +7 years	DESTROY
Disciplinary proceedings:			
Disciplinary – Oral warning		Date of warning + 6 months	DESTROY
Disciplinary – Written warning – level one		Date of warning + 6 months	DESTROY
Disciplinary – Written warning – level two		Date of warning + 12 months	DESTROY
Disciplinary – Final warning		Date of warning + 18 months	DESTROY
Records relating to incidents/injury at work		Date of incident + 12 years	Review at the end of this period. In the case of serious accidents, a further retention period will need to be applied.
Staff appraisal/ Performance management		Current year + 5 years	DESTROY
Interview notes and recruitment records		Date of interview + 6 months	DESTROY
Pre-Employment information + DBS		Destroy after processing	DESTROY
Timesheets, sick pay		Current year + 6 years	DESTROY
Training Records		Termination + 7 years	DESTROY & DELETE



Administrative

	Statutory Provision	Retention Period	Action at end of the administrative life of the record
Employer's Liability certificate		Permanent whilst the school is open	DESTROY once the school has closed
School brochure/prospectus		Current year + 3 years	
Newsletters		Current year + 1 year	Review to see if a further retention period is required.
Visitor's book		Current year + 2 years	Review to see whether a further retention period is required.

Finance

	Statutory Provision	Retention Period	Action at end of the administrative life of the record
Annual Accounts	Financial Regulations	Current Year + 6 years	
Loans & Grants	Financial Regulations	Date of last payment on loan + 12 years	
Contracts		Contract completion date + 6 years	
Copy orders		Current year + 2 years	
Budget reports, budget monitoring etc		Current year + 3 years	
Invoice, receipts and other records covered by the Financial Regulations	Financial Regulations	Current year + 6 years	
Annual budget and background papers		Current year + 6 years	
Debtors' records	Limitation Act	Current year + 6 years	
Applications for free school meals, travel, uniforms etc.		Whilst child is at school	
Student grant applications		Current year + 3 years	
Free School Meal registers	Financial Regulations	Current year + 6 years	
Petty cash books	Financial Regulations	Current year + 6 years	

Appendix 2: Privacy notice for parents/guardians

Headteacher: Mr J Evans



HERONSBRIDGE SCHOOL

Ewenny Road, Bridgend CF31 3HT

Tel: (01656) 815725 Fax: (01656) 815729

Email: admin.heronbridge@bridgend.gov.uk

Privacy Notice for Parents/Guardians

This privacy notice explains why we need pupil information and what we do with it.

A new law

There are rules on how to keep information safe and how it is shared. These rules are in **The Data Protection Act 1998**. In 2018, there is a new law called the **General Data Protection Regulation (GDPR)**. It gives you more control over your information. It makes sure anyone collecting information has to:

- Be honest about why they want it
- Be clear about what they will do with it

Your Information

Schools collect information about pupils and their parents/guardians/families and share the information with the relevant local authority, Welsh Government and other statutory authorities.

The categories of information about pupils that we collect, hold and share include:

- Personal information (such as name, date of birth, unique pupil number, unique learner number and address)
- Relationships (such as names of parents/guardians and any other relatives or contacts that are provided to the school) and contact details
- Characteristics (such as ethnicity, first language, nationality, country of birth, religion and free school meal eligibility)
- The pupil's level of fluency in the Welsh language and how this has been assessed/provided
- Medical conditions / information (such as allergies)
- Disability status
- School history
- School transportation
- Registration status and full-time or part-time status
- Information on additional learning needs
- Information on whether the pupil is in the care of the local authority
- Information on whether the pupil is receiving support from other agencies
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Educational attainment and assessments
- Any issues or problems arising at school and actions taken in response (such as behavioural issues, exclusions etc.)
- Counselling information/records
- Financial information (such as school meal balance)
- Images, which may include photographic images and CCTV images

Why we collect and use this information

We use the pupil information:

- To support pupil learning
- To monitor and report on pupil progress
- To provide appropriate pastoral care
- To assess the quality of our services
- To comply with the law
- To keep people safe

The lawful basis on which we use this information

We collect and use pupil information under the **Education Act 1996 and associated regulations.**

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, **we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.**

Storing pupil data

We hold pupil information until the pupil reaches his/her 25th birthday.

Who we share pupil information with

We routinely share pupil information with:

- Other schools/settings that pupils attend
- Bridgend County Borough Council
- Welsh Government and agencies acting on its behalf
- The Central South Consortium (this is the regional education consortium)
- Examination/Accreditation Boards
- Health providers and other statutory agencies
- Careers Wales
- The Police

Why we share pupil information

We do not share information/data about our pupils with anyone without consent unless the law and our policies allow us to do so. We are required to share information about our pupils with Bridgend County Borough Council and Welsh Government. We share pupil information with Welsh Government and agencies acting on its behalf on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

Your rights

Requesting access to your personal data

Under data protection legislation, parents/guardians and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or to be given access to your child's educational record, please contact the Headteacher.

You have the right to:

- See any personal information we have about you
- Ask us to change any information that you think is wrong
- Ask us to not share your information, but this will not apply when we need to get support for the pupil or keep the pupil safe
- Ask us to remove information from our systems.

Pupils (subject to certain limitations) and parents/guardians also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress
- Prevent processing for the purpose of direct marketing
- Object to decisions being taken by automated means
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed
- Claim compensation for damages caused by a breach of the Data Protection regulations

You can complain if you think we are not respecting your rights.

You can seek help from the Information Commissioner's Office (ICO). The contact details are:

Information Commissioner's Office

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: **01625 545 745** or **0303 123 1113**

www.ico.gov.uk

Contact

If you would like to discuss anything in this privacy notice, please contact the Head Teacher.

Appendix 3: Privacy notice for school workforce



Headteacher: Mr J Evans

HERONSBRIDGE SCHOOL

Ewenny Road, Bridgend CF31 3HT

Tel: (01656) 815725 Fax: (01656) 815729

Privacy Notice for School Workforce

This privacy notice explains why we need school workforce information and what we do with it. The school workforce encompasses those employed to teach, or otherwise engaged to work, at the school.

A new law

There are rules on how to keep information safe and how it is shared. These rules are in **The Data Protection Act 1998**. In 2018, there is a new law called the **General Data Protection Regulation (GDPR)**. It gives you more control over your information. It makes sure anyone collecting information has to:

- Be honest about why they want it
- Be clear about what they will do with it

Your information

The categories of school workforce information that we collect, process, hold and share include:

- Personal details, such as name, date of birth, employee or teacher number, national insurance number, address
- Special categories of data relating to equalities and Welsh language such as gender, age, ethnicity group, disability and Welsh language skills
- Job applications and references
- Outcomes of DBS checks
- Health and safety information
- Employee and emergency contact information and next of kin details
- Contract information, such as start dates, hours worked, post, Payroll information, such as salary, HMRC information and pension details
- Absence information, such as number of absences and reasons, medical certificates
- Qualifications (and, where relevant, subjects taught) and training information
- Information on matters arising from your employment and actions taken in response
- Vehicle information
- Driver's license details (if driving school minibuses)

Why we collect and use this information

We use school workforce data to:

- Enable the development of a comprehensive picture of the workforce and how it is deployed
- Inform the development of recruitment and retention policies
- Enable individuals to be paid
- Support and manage employees
- Recruit and select employees
- Ensure eligibility to drive school transport covered by valid insurance

The lawful basis on which we process this information

As your employer we need to process your personal data in order to: fulfil our contractual obligations to you and other legal obligations. This is our lawful basis for processing under the GDPR.

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, **we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.**

Storing this information

We hold school workforce data for seven years after employment has ceased.

Who we share this information with

We share this information with the following bodies when required and in accordance with our legal obligations:

- Bridgend County Borough Council
- Local and central government
- Regulatory bodies
- Prospective employers
- Professional bodies
- Pension administrators
- Training providers
- Auditors
- DBS

Why we share school workforce information

We only share information about employees when the law and our policies allow us to do so.

Bridgend County Borough Council

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (Wales) Regulations 2017 and any associated amendments.

Welsh Government

We share personal data with Welsh Government on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

Your rights

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the Headteacher and the Principal Advisor Employee Relations – Schools, or the Workforce Planning and Administrative Manager, in the Human Resources Department at Bridgend County Borough Council.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can seek help from the Information Commissioner's Office (ICO). The contact details are:

Information Commissioner's Office

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: **01625 545 745** or **0303 123 1113**





www.ico.gov.uk

Further information

If you would like to discuss anything in this privacy notice, please contact the Head Teacher

Appendix 4

Information and Data Categories

Type of Information	Description	Risk level	Examples
Public 	Publicly available information	None	Website content, research, Curriculum Frameworks,
Unrestricted 	Information that is not in the public domain but contains no personal data. Disclosure of information is not advisable but is of low risk.	Low	Policies, Schemes of work, Correspondence templates, General Photos/videos*
Restricted 	Personal information which could cause discomfort or harm if disclosed.	Medium	IEAs, Annual Reports, PCPs, Assessments, Photos/video with personal information.
Highly Restricted 	Sensitive personal data (Special category data-see Data Protection policy).	High	Statements, Annual Reviews, Provision map

*Photos/videos with no other additional information attached, including names/class/age