Ysgol Plas Brondyffryn
Data Protection Policy

Forward by the Headteacher

In delivering its services Ysgol Plas Brondyffryn will need to collect and process certain types of information about people including school staff, school pupils and suppliers or providers of services to it. All such processing is subject to the General Data Protection Regulation (GDPR) and the more particularly the Data Protection Act 2018. This policy sets out the School's intentions in fulfilling its obligations under this legislation.

The School needs to keep personal information secure, but it goes much wider than appropriate security and requires a comprehensive approach to the collection, use, sharing and retention of personal information, in order to build public confidence. Combined with the reliance on fast changing ICT capabilities and storage of vast amounts of data, it is essential that the School has this overarching document in plain language, which makes clear to the public the School's approach to data protection and data sharing; and explains the rights of the individual in relation to the information we hold about them. Publishing a clear and explicit policy and having the right approach to raising awareness and skills of staff, as they handle personal information, will be regarded as an integral element in promoting trust in the way this School handles the personal data entrusted to it.

We have all been made aware of high profile data breaches, and many will be will be aware of the Information Commissioner's powers to fine authorities up to 10 million euros for severe breaches. Many of the reported breaches are however simply down to human error, such as inputting the incorrect fax number, emailing the wrong recipient or not checking personal data before it is posted, leaving sensitive documents in the car or not checking a person's identity over the phone. These errors can all be avoided by officers and members taking extra care in going about their duties and treating others' personal information, as they would their own. The school's leadership team and Governing Body also have an important role to play in proper oversight of its systems and processes so it makes breaches less likely.

In addition, in respect of any data processing generally, I am pleased to sign off a 'Personal Information Promise' - it is a form of mission statement for the handling of personal information aimed at those whose personal information we hold. If a compliance problem occurs we will reflect on whether we are living up to this promise, and I urge all staff to read this promise as it puts the Data Protection Act 2018 obligations into straightforward language that we can all understand and put into practice.

PERSONAL INFORMATION PROMISE

I, Jane Bryant, Headteacher, on behalf of Ysgol Plas Brondyffryn promise that we will:

1. Value the personal information entrusted to us and make sure we respect that trust;

2. Go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;

3. Consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;

4. Be fair, open and transparent with individuals about how we use their information and who we give it to;

5. Make it easy for individuals to access, correct and request erasure (where we have no reason to retain), of their personal information;

6. Keep personal information to the minimum necessary and delete it when we no longer need it;

7. Have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;

8. Provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly;

9. Put appropriate resources into looking after personal information to make sure we can live up to our promises; and

10. Regularly check that we are living up to our promises and report to the Governing Body and any external regulators on how we are doing.

Signed:

Dated:

Introduction
Ysgol Plas Brondyffryn shall at all times comply with its duties under the Data Protection Act 2018 and the rights of privacy and respect for personal and family life set out in Article 8 of the Human Rights Act 1998.

The Data Protection Act 2018 (the Act) places legal obligations on organisations who collect and use personal information and gives individuals certain rights. In addition, there are stricter requirements in the Act in respect of processing 'special category data'. Personal information can be held in any format e.g. electronic, paper records, CCTV or photographic images and the Act applies, irrespective of how the information is held.

Responsibility for the Act
The School is committed to ensuring all staff and contractors comply with the Act. The School has an appointed Data Protection Officer who is responsible for ensuring compliance with the Act.

There is a separate policy in respect of the Freedom of Information Act and the Environmental Information Regulations. Where a request is received under the FOIA or the EIRs but in fact it falls within the Data Protection regime, the School will automatically channel it through the appropriate policy, as it is required to do, as different exemptions and therefore, different legal rights apply in the circumstances.

Scope
This policy applies to all personal information held in any recorded format such as email, paper, video, CCTV or photographic images and applies to all staff and governing body members who process personal data on behalf of the school. It is a criminal offence to destroy personal information when the purpose of the destruction was to avoid disclosure following a request.

Adhering to the 6 principles of the Act
The Data Protection regime is underpinned by 6 certain fundamental principles, which form a code for the proper processing of personal data. Processing means anything we do with data; such as obtaining, copying, disclosing, altering, retaining or destroying information. If we cannot comply with all these 6 principles, we should not be processing the data. The principles are summarised below –

1. Personal data must be lawfully, fairly and transparently processed.

2. Personal data shall be collected for specified, explicit and legitimate purposes.

3. Personal data shall be adequate, relevant and limited to what is necessary.

4. Personal data must be accurate and up to date.

5. Personal data shall be kept in a form which permits identification for no longer than necessary.

6. Personal data shall be held ensuring appropriate security.

The School will ensure that: -

- It has in place procedures for complying with the six principles.

- Training on our data protection duties shall be mandatory for all staff. All new staff receive appropriate data protection training on induction and that refresher training and guidance is provided periodically, so that they understand that they are contractually responsible for complying with the law and know how to process information in accordance with these 6 principles.

- Advanced level training is provided to those members of staff who deal with highly sensitive personal information, such as the Special Educational Needs Co-Ordinator. Training needs mapping will be conducted, to identify those who require regular advanced training on data protection and information sharing, to enable them to share with confidence.

- Everyone managing and handling personal information are individually and collectively responsible for compliance with this policy.

- A failure to follow this policy may result in disciplinary action or even criminal prosecution in the case of a wilful and deliberate breach.

- That individuals are informed of the purposes for which their data will be used and that consent is sought for such use, where required under the Act. Examples of model privacy notices are attached as an appendix to this policy.

- All staff are trained to recognise a subject access request and what to do about one.

- All appropriate, technical and organisational security measures to safeguard personal information will be put in place including encrypting or ensuring increased security settings of removable devices such as laptops or mobile phones and restricting the use of USB sticks in line with the School's Information Security Policy.

- All staff are required to report data security breach incidents, including 'near misses' to their line manager who shall inform the Headteacher immediately.

Individual's Rights
The School will ensure that individuals can exercise their rights as set out in the Act including:-

- the right to be informed of the purposes of the processing;
- the categories of personal data being processed;
- the right of subject access to their personal information;
- who will or is likely to receive their information;
- the envisaged period for which the data will be stored;
- the right to prevent processing of personal information in certain circumstances;
- the right to rectify, block, erase, restrict, object or correct inaccurate information;
- the right to lodge a complaint;

These rights apply to all living, identifiable individuals on whom the School processes personal information.

Subject Access Requests

Article 15 of the GDPR provides the right for individuals to be told by the Data Controller (the organisation who determines the purposes for which and the manner in which personal information is processed)

- if we hold information about them,
- to ask what we use it for,
- to be given a copy of the information,
- to be given details of other organisations or people we disclose it to,
- to ask for incorrect data to be corrected,
- to ask us not to use personal information about them for direct marketing,
- to be compensated for damage or distress if we do not comply with the Act,
- to object to decisions made only by automatic means – for example where there is no human involvement,
- to ask the Information Commissioner's Office to investigate and assess whether we have breached the Act.

The School will supply this information providing the request is made verbally or in writing, and it is sufficiently clear what personal information is being sought; therefore sufficient information should be given by the applicant to enable the School to locate the information requested.

There is no fee applicable and the School should respond within one month, unless the request is complex or multiple, in which case it may be extended by two further months. The School will inform the applicant if it is extending the time frame in such circumstances setting out the reasons as to why.

The School will respond to such requests within one month, unless the request is manifestly unfounded or excessive. There is no definition within the Act, but in respect of an 'excessive' request, it is generally taken to mean that the effort the organisation would have to expend in complying with the requirement to provide a copy, is disproportionate to the benefit to be derived by the individual in receiving it. In such circumstances the School will refuse the request.

Advice should be sought from the School's Data Protection Officer in the first instance, ideally before the School commence their search and collation of the data.

Where the individual makes a request electronically, the School will provide the information in a 'commonly used electronic format' in accordance with the GDPR; unless the applicant requests otherwise.

A request for personal information should be submitted to the following contact:
Sian Dent (ICT/Data Manager) - post@ypbd.co.uk

What if the data includes information about other people?
Applicants will not automatically be given access to parts of their information which also identify other people, without that third party's agreement, even if they are related. Disclosure will depend on the context and whether information is already within knowledge and all the circumstances of the case. Seek advice if in doubt.

The Act says that the School would not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information, the School must take into account all of the relevant circumstances, including:

- the type of information that would be disclosed;
- any duty of confidentiality owed to the other individual;
- any steps taken to seek consent from the individual;
- whether the other individual is capable of giving consent;
- any express refusal of consent by the individual.

These are areas should be taken into account, but they are not necessarily determinative, as the decision is one for the School to make, balancing the data subject's rights against other individual rights.

This does not apply to school staff and governing body members or other professional officers, whose name may appear within a person's information, it is expected that this will be disclosed unless there is a risk of 'serious harm'. The serious harm test is a legal test and advice should be sought. The GDPR provides that it is expected that school professionals will be disclosed.

What about requests for information about children or young people?[1]

All the rights set out in the paragraph above are equally applicable. However, it should be remembered that even if a child is too young to understand the implications of the subject access rights, it is still the right of the child rather than anyone else such as a parent or guardian. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility.

Before responding to a subject access request for information held about a child, the School should consider whether the child is mature enough to understand their rights. If the School is confident that the child can understand their rights, it should respond directly to the child. The School may however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, the School should take into account, (in no particular order) among other things:

- the childs' level of maturity and their ability to make decisions like this,
- the nature of the personal data,
- any court orders relating to parental access or responsibility that may apply,
- any duty of confidence owed to the child or young person,
- any consequences of allowing those with parental responsibility access to the child's or young persons' information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information;
- any views of the child or young person has on whether their parents should have access to information about them.

In Scotland there is a presumption that a person 12 years and over is of sufficient age and maturity, unless the contrary is shown. The law in Wales does not specify an age and competence is assessed depending on the level of understanding of the child, but it does indicate an approach that will be reasonable.[2]

Exemptions

The School may also under the Act and Article 15 GDPR refuse disclosure of data under the right of access provisions, where the serious harm test is met in respect of disclosure of education data.

[1] Extracted from the ICO guide to the GDPR 22nd March 2018.

[2] The test on Gillick competency is also helpful in the context of data protection requests.

Information Sharing

Information sharing is a complex area spanning many statutes and often the detail is hidden in secondary legislation (such as orders or statutory instruments). Decisions on whether to share information must be taken on a case-by-case basis and there could not be a blanket policy statement to follow as this is likely to be unlawful. In addition, understanding what can legally constitute 'consent', is also fundamental.

However, the following statements should clarify previous common myths or misunderstandings regarding information sharing:

The Data Protection Act does not prevent, neither should it be seen as a barrier, to lawful information sharing.

The School is not legally required to have an 'Information Sharing Protocol' in place, in order to share. The lack of an ISP should not be a reason for not sharing information that could help a practitioner deliver services to a person.

Some Schools have signed up to the Wales Accord on the Sharing of Personal Information (WASPI), however not every information sharing arrangement will need to be WASPI approved.

Consent is not a prerequisite to information sharing – but several legal regimes (including the Data Protection Act) confirm that the obtaining of valid consent will permit information to be shared lawfully, but you may be able to rely on other grounds to share rather than obtain consent.

Confidentiality you may owe to an individual, can, and in some circumstances, *must* be overridden, such as concerns that a vulnerable adult or child may be at risk of serious or significant harm. Follow the relevant procedures without delay.

Over the page are seven golden rules for information sharing reproduced from the HM Government publication 'Information Sharing; Guidance for practitioners and managers'. These rules compliment the Welsh Government's WASPI principles that the School may have signed up to; Denbighshire County Council has signed up to WASPI and supports Denbighshire Schools to also do so. The golden principles below are equally relevant in Wales and provide school staff with clear guidelines when they decide to share information.

Seven golden rules for information sharing

1. Remember that the Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately

2. Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. Seek advice if you are in any doubt, without disclosing the identity of the person where possible.

4. Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.

5. Consider safety and well-being: Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

6. Necessary, proportionate, relevant, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Requests from third parties (e.g. the Police) for an individual's personal information

Occasionally the School may receive formal requests under the Act from other agencies or third parties such as the police, DWP or HMRC, solicitor's firms etc., to physically access or receive a copy of the information relating to an individual. These sections do not provide the School with an automatic reason to disclose, as is explained below.

The Act deals with several situations in which personal data is processed for the following 'crime and taxation' purposes:

- the prevention or detection of crime;
- the capture or prosecution of offenders; and
- the assessment or collection of tax or duty.

The personal data could be disclosed if the disclosure is for any of the above crime or taxation purposes and the above purposes are 'likely to be prejudiced' if the School did not disclose e.g. to the police or the Inland Revenue. The threshold for disclosure in these circumstances needs to be more than a mere risk of prejudice and needs to be a significant and weighty chance of prejudice to the above purposes. In such circumstances you would need the third party to set out what information they wanted to see (or envisaged) and what legal powers they are relying on and evidence of identity. Seek advice from the School's Data Protection Officer or legal services if in doubt.

Disclosure of personal information over the telephone or face to face without establishing the identity of the recipient should be avoided.

What about our external suppliers and the School outsourcing personal data processing?

The School uses third party organisations to perform some of its functions. Where such 'outsourcing' arrangements involve the processing of personal data, certain legal obligations are placed on the school to ensure this supplier looks after the personal information in the same secure way as the School does. These obligations are more onerous now under GDPR than under the old data protection legislation therefore extra care needs to be taken when entrusting a third party supplier with personal data. Seek advice if you are in doubt. Follow your Schools Purchasing Rules (or Contract Procedure Rules).

It is legal requirement that the obligations imposed on the supplier (known as the data processor) be set out in a written contract or letter. The Council's Standard Corporate Terms and Conditions should used – these are available from the Council's Corporate Procurement Unit – the obligations are already set out in these standard contracts so you know you will be covered. The Procurement Unit may identify a framework that is already set up and the contract terms are already included and suppliers vetted.

Introduction of new systems that affect personal information – what should the School consider?

In developing information systems or new business processes or changes to our existing processes, that involve personal information, it is now a requirement to carry out a Data Protection Impact Assessment (DPIA) and to build in privacy-friendly solutions as part of modernising or introducing new systems. This is referred to under the GDPR as 'Privacy

by Design and Default' and the DPIA can be a useful tool to help identify risks and help the School manage those risks and where possible eliminate them.

The Council has standard templates for carrying out DPIAs so you have an audit trail of how you have considered the impact of the new system on people's personal data. These are available on the Business Improvement and Modernisation section of the intranet.

Email use

School staff should only use an authorised email account to communicate in respect of school business and functions. Under no circumstances should school staff (including fixed term, temporary, supply, agency or otherwise) use their personal email account to communicate with pupils, in order to protect all individuals concerned. Any staff member communicating in breach of this policy may face disciplinary action.

Data Security Breaches

All data security breaches, including 'near misses', must be reported to the Line Manager responsible, who shall immediately inform the Headteacher who shall advise on the necessary steps that need to be taken to contain any resultant damage and inform individuals who may be affected. A central record of all breaches will be retained and serious breaches must now be reported to the Information Commissioner's Office. There is a standard breach notification form on their website. The School's Data Security Breach policy should be consulted.

Oversight arrangements and review of policy

This policy will be reviewed no later than December 2021. Compliance with this policy and related procedures will be monitored by the School Leadership team and the Governing Body.

Complaints

A review of the School's decision to *withhold* personal information where an applicant has made a subject access request, can be made to the School's Data Protection Officer who will facilitate a review. If the decision is upheld, and the applicant remains unsatisfied they may appeal to the Information Commissioner's Office.

Contact details

Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel 01625 545745
www.informationcommissioner.gov.uk

Key Contact details:

- Wales Accord on the Sharing of Personal Information
  The WASPI team is currently hosted by the health authority and their contact details are available on their website www.waspi.org

- Joint Corporate Procurement Unit
  Legal, HR and Democratic Services
  Level 2
  County Hall
  Ruthin
  Denbigshire
  Telephone number:
  Email:

- Subject Access Requests: Sian Dent (ICT/Data Manager)
  Email: post@ypbd.co.uk

Appendix 1

Privacy Notice

The categories of pupil information that we process include the following non-exhaustive list:

- personal identifiers and contacts (such as name, unique pupil number, contact details and address)
- characteristics (such as ethnicity, language, and free school meal eligibility)
- safeguarding information (such as court orders and professional involvement)
- special educational needs
- medical and administration (such as doctors information, child health, dental health, allergies, medication and dietary requirements)
- attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- assessment and attainment (such as post 16 courses enrolled for and any relevant results)
- behavioural information (such as exclusions and any relevant alternative provision put in place)
- information about attendance on school trips and activities (safety issues and risks for keeping a pupil safe, emergency contact details; next of kin)
- food allergies (for catering)

Why we collect and use pupil information

We collect and use pupil information, for the following purposes:

a) to support pupil learning
b) to monitor and report on pupil attainment progress
c) to provide appropriate pastoral care
d) to assess the quality of our services
e) to keep children safe (food allergies, or emergency contact details)
f) to meet the statutory duties placed upon us by the Welsh Government with regard to data collection.
g) to communicate effectively with parents and carers.
h) to enable pupils to move from one educational setting to another seamlessly, or where we have co-operation arrangements with other schools, for delivery of local curricular entitlements.

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing pupil information will usually be the following:

- As data controller, the School uses the information received for the purposes listed above to enable us to carry out data processing necessary for the performance of a task carried out in the public interest and in the exercise of official authority or where we have a legal obligation to process.
- In addition, concerning any 'special category data', where the processing is necessary for reasons of substantial public interest; or where we have obtained explicit consent.

How we collect pupil information
We collect pupil information via admission forms or registration forms completed at the start of school years; via 'common transfer files', or file transfer from a previous school. Pupil data is essential for the schools' operational use. Whilst the majority of pupil information you provide to us is mandatory, some of it requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this.

How we store pupil data
We hold pupil data securely for the set amount of time shown in our data retention schedule. For more information on our data retention schedule and how we keep your data safe, please visit the school website for the latest information. We are required to retain certain educational information until a pupil's 25th birthday for example.

Who we share pupil information with
We routinely share relevant pupil information with:

- schools that the pupils attend after leaving us
- our local authority
- Welsh Government
- NHS /school nurse; either directly or via the local authority such as for immunisation programmes.

Why we regularly share pupil information
We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so. Where appropriate we will aim to have a formal Information Sharing Protocol in place and have made a commitment to developing these in accordance with national standards laid down by the Welsh Government's Wales Accord on the Sharing of Personal Information (WASPI) see www.waspi.org

Youth support services
We also pass pupil information to our local authority and / or providers of youth support services, under the Learning and Skills Act 2000 and the Learning and Skills (Wales) Measure 2009, as they have responsibilities in relation to the education or training; from aged 11 to 19.
This enables them to provide services as follows:

- youth support services
- careers advisers
- post 16 education and training providers

The information shared is limited to the child's name, address and date of birth. However where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child / pupil once they reach the age 16 under the Learning and Skills Act 2000 (s.126 (2)).
Data is securely transferred to the youth support service and held for in accordance with the Data Protection Act 2018. The receiving organisation eg Careers Wales, will then become the Data Controller in respect of the sent information and will provide you with any privacy or fair processing information directly.

Welsh Government
The Welsh Government collects personal data throughout a pupil's school life from educational settings and local authorities via various statutory data collections such as:

- Pupil Level Annual School Census (PLASC)
- Educated other than at school (EOTAS) pupil level collection
- National data collection (NDC)
- Attendance collection
- Welsh National Tests (WNT) data collection
- Post 16 data collection

In addition to the data collected as part of PLASC, the Welsh Government and Local Authorities also receives information regarding National Curriculum assessments, public examination results, and attendance data at individual pupil level which comes from Schools and /or Awarding Bodies (e.g. WJEC).

We are required to share information about our pupils with the Welsh Government either directly or via our local authority for the purpose of those data collections, under The Pupil Information (Wales) Regulations 2011.

Why do we share this data with the Welsh Government?
The pupil data that we lawfully share with the Welsh Government through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures).
- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

All data is transferred securely and held by the Welsh Government under a combination of software and hardware controls.

For more information please visit the Welsh Government website on www.gov.wales/School Data and in particular the privacy notice entitled:
What we do with the education related information that we receive from schools and/or local authorities about children and young people.

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

In certain circumstances 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
- a right to seek redress, either through the ICO, or through the courts

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns

Contact
If you would like to discuss anything in this privacy notice, please contact: Data Protection Officer for Schools, whose contact details are:

Lisa Jones, Legal Services Manager on **dataprotection@denbighshire.gov.uk**
Legal, HR and Democratic Services, Denbighshire County Council, County Hall, Ruthin, Denbighshire. LL15 1YN
Tel: 01824 706275

Policy adopted:	Summer 2015
Reviewed:	Summer 2016
Reviewed:	May 2019
To be reviewed:	May 2021

Equality Impact Assessment completed
An Equality Impact Assessment offers an opportunity for staff to think carefully about the impact of their work on local people and other members of staff.
Date completed:
June 2016