General Data Protection Regulation (GDPR) Policy

Ysgol Bryn Castell

Approved By: Governing Body May 6th, 2025

Last reviewed on: 12/03/25

Next review Due Spring Term 2027 (or when a legal change / update is required)

The United Nations Convention on the Rights of the Child (UNCRC) is the most complete statement of children's rights ever produced and is the most widely-ratified international human rights treaty in history. This policy relates to Article 16 of the UNCRC.

Article 16: Children have a right to privacy. The law should protect them from attacks against their way of life, their good name, their families and their homes.

Ysgol Bryn Castell Special School is a Rights Respecting School.

As a Rights Respecting School, we aim to embed children's human rights in our ethos and school culture. We base our practice on the principles of equality, dignity, respect, non-discrimination and participation. Working within these principles not only empowers our children and young people, but also leads to enhanced learning, improved standards and better relationships.

1. **General Data Protection Regulation (GDPR) Policy**

The UK General Data Protection Regulation (UK GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

Ysgol Bryn Castell Special School collects and uses personal information about staff, pupils, parents and other individuals who come in contact with the school. The information is gathered in order to enable the school to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure the school complies with its statutory obligations.

The school has a duty to inform individuals including parents and pupils of the information that it holds. This policy document should summarise why the data is held and any other parties to whom this information may be passed on to.

2. Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely in line with General Data Protection Regulations (GDPR). It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed and irrespective of whether it is held in paper files or electronically.

3. Our Commitment:

The school is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the General Data Protection Regulations.

4. Legal Basis

Changes to data protection legislation (GDPR May 2018) shall be monitored and implemented in order to remain compliant with all requirements. The legal bases for processing data are as follows:

- You must have a valid lawful basis in order to process personal data.
- There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.
- Most lawful bases require that processing is 'necessary'. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.
- You must determine your lawful basis before you begin processing, and you should document it. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason.
- Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.
- If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).
- If you are processing special category data, you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.
- If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

5. Personal and Sensitive Data:

The school has a data map which details all data in use across the school. All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

- Personal data only includes information relating to natural persons who:
    - can be identified or who are identifiable, directly from the information in question; or
    - who can be indirectly identified from that information in combination with other information

The principles of GDPR shall be applied to all data processed and are underpinned by 7 enforceable principles: The GDPR sets out seven key principles:

    - Lawfulness, fairness and transparency

- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

6. Roles and Responsibilities

The members of staff responsible for data protection are:

- Sean Jenks– Senior Data Protection Co-ordinator
- Helen Ridout – Headteacher
- Kaye Cheeseman –Admin Manager
- Philip Aubrey - Chair of Governors

GDPR is a collective responsibility and all staff must treat all personal/sensitive information in a confidential manner and follow the guidelines as set out in this document. The school is also committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them through our training programme. The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

7. Notification:

We are registered with the information Commissioner's office (ICO) as required of a recognised Data Controller that processes personal information. Details are available from the ICO. https://ico.yk/what-we-do/register-of-fee-payers

8. Individuals' Rights

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

9. Privacy Notice:

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data.

Notifications shall be in accordance with ICO guidance and where relevant, be written in a form that is understandable by those defined as 'Children' under the legislation:

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form t understandable by those defined as 'Children' under the legislation. Transparency (cookies and privacy notices) | ICO /

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example Welsh Government, local authorities, ESTYN, or University Health Board. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect. The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

For further details please see our privacy notices which can be located on our website

10 Data Security:

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them. Risk and impact assessments shall be conducted in accordance with guidance given by the ICO.

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.
The security arrangements of any organisation with which data is shared shall also be considered and where required, these organisations shall provide evidence of the competence in the security of shared data.

11.Subject Access Requests:

All individuals whose data is held by us, have a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to:

Helen Ridout,

Headteacher,

Ysgol Bryn Castell

Bryncethin Campus

Abergarw Road

Bridgend

CF32 9NZ

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child.

Data may be disclosed to the following third parties without consent:

- **Other schools**
  If a pupil transfers from our school to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. This will aid continuation, which should ensure that there is minimal impact on the child's academic progress as a result of the move

- **Examination authorities**
  This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

- **Health authorities**
  As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

- **Police and courts**
  If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

- **Social workers and support agencies**
  In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

- **Educational division**
  Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

- **Right to be Forgotten**
  Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

12. Location of information and data:

Electronic Records

The use and storage of personal/sensitive data in electronic/digital format is explained in the online safety policy. The use of data in electronic/digital form is bound by the 7 principles of the GDPR. The school's main electronic platform is SIMS. The school also uses Teachers 2 Parents for its communication with parents, EVOLVE for planning Educational Visits, SLEUTH for behaviour tracking, MyConcern for Safeguarding issues, Motional to help to support the emotional development of our young people, Provision Map to map and manage provision for the pupils, the Hwb and Google Applications for curriculum resources. All platforms are accessed by passwords which are suitably complex. All platforms should be shut down after each use.

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. The only exception to this is medical information, individual education plans and positive handling plans that may require immediate access during the school day.

Sensitive or personal information/data should not normally be removed from the school site. However, the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings or are on school visits with pupils. Reasonable precautions should be taken to safeguard the information.

If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.

If it is necessary to transport data away from the school, it should be downloaded onto a school supplied, encrypted USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB and saved onto the USB only.

USB sticks that staff use must be password protected and supplied by the school. These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Individuals' network areas should be regularly maintained and de-cluttered to ensure no unwanted duplication.

Paper Records

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.

- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.

13. Data Disposal:

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance:

Records management and security | ICO

The school has identified a qualified source for disposal of IT assets and collections.

The school also uses high quality shredders to dispose of paper assets.

14. Breaches of GDPR

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. This will be done within 72 hours of the school becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the school will inform those individuals without undue delay.
- The school has robust breach detection, investigation and internal reporting procedures in place – these are at Appendix 1 of this policy
- The school will keep a record of any personal data breaches, regardless of whether you are required to notify.

Further Information

Information Commissioners Office – www.ico.org.uk

Appendices

- Appendix 1 – Breach Notification Procedure
- Appendix 2 – Mobile Technologies and Working from Home including Bring Your Own Device.
- Appendix 3 Staff, Governors Acceptable Use Agreement:
- Appendix 4 - Privacy Notice (Parents, Guardians, Pupils)

Appendix 1: Breach Notification Procedure

Helen Ridout has overall responsibility for breach notification within the School. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.

The Data Protection Officer (DPO) is responsible for overseeing this policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this policy or the GDPR or if you have any concerns that this policy is not being or has not been followed.

The DPO contact details are set out below:-

Data Protection Officer: Craig Stilwell

Address: Judicium Consulting Ltd. 5th Floor, 98 Theobalds Road, London WC1X 8WB

Email: dataservices@judicium.com

Telephone 0345 548 7000

What Is A Personal Data Breach?

A personal data breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive):-

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss)
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error (for example sending an email or SMS to the wrong recipient)
- Unforeseen circumstances such as a fire or flood.
- Hacking, phishing and other “blagging” attacks where information is obtained by deceiving whoever holds it.

When Does It Need To Be Reported?

The School must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of the individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes:

- Potential or actual discrimination.

- Potential or actual financial loss.
- Potential or actual loss of confidentiality.
- Risk to physical safety or reputation.
- Exposure to identity theft (for example through the release of non-public identifiers such as passport details).
- The exposure of the private aspects of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of the individuals then the individuals must also be notified directly.

Reporting A Data Breach

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should: -

- Complete a data breach report form.
- Email the completed form to the DPO.

Where appropriate, you should liaise with your line manager about completion of the data report form. Breach reporting is encouraged throughout the School and staff are expected to seek advice if they are unsure as to whether the breach should be reported and /or could result in a risk to the rights and freedom of individuals. They can seek advice from their line manager, Helen Ridout or the DPO.

Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further.

Managing and Recording the Breach

On being notified of a suspected personal data breach, the School will notify the DPO. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps to:-

- Assess and record the breach in the School's data breach register.
- Notify the ICO.
- Notify data subjects affected by the breach.
- Notify other appropriate parties to the breach.
- Take steps to prevent further breaches.

Notifying the ICO

The School will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of school holidays (i.e. it is not 72 working hours). If the School are unsure of whether to report a breach, the assumption will be to report it.

Where notification is not made with 72 hours of becoming aware of the breach, written reasons will be recorded to why there was a delay in referring the matter to the ICO.

Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the School will notify the affected individuals without undue delay including the name and contact details of the DPO and the ICO, the likely consequences of the data breach and the measures the School have (or intend) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, the School will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police)

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the School will consider alternative means to make those affected aware (for example by making a statement on the School website)

Notifying Other Authorities

The School will need to consider whether other parties need to be notified of the breach for example:

- Insurers
- Parents
- Third parties (for example when they are also affected by the breach)
- Local authority
- The Police (for example if the breach involved theft of equipment or data)

This list is non-exhaustive.

Assessing The Breach

Once initial reporting procedures have been carried out, the School will carry out all necessary investigations into the breach.

The School will identify how the beach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover, correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data)

Having dealt with containing the breach, the School will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and /or data subjects as set out above). These factors include:-

- What type of data is involved and how sensitive it is.
- The volume of data affected
- Who is affected by the breach (i.e. the categories and number of people involved)
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise.
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation)
- What has happened to the data
- What could the data tell a third party about the data subject
- What are the likely consequences of the personal data breach on the school; and
- Any other wider consequences which may be applicable.

Preventing Future Breaches

Once the data breach has been dealt with, the School will consider its security processes with the aim of preventing further breaches. In order to do this, we will:-

- Establish what security measures were in place when the breach occurred
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice
- Consider whether it is necessary to conduct a privacy or data protection impact assessment
- Consider whether further audits or data protection steps need to be taken
- To update the data breach register
- To debrief governors/ management following the investigation.

Reporting Data Protection Concerns

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they do not meet the criteria of a data breach) that you may have to Helen Ridout or the DPO. This can help capture risks as they emerge, protect the School from data breaches and keep our processes up to date and effective.

Appendix 2: - Mobile Technologies and Working from Home including Bring Your Own Device

A key strategic aim of Ysgol Bryn Castell is to promote an effective work life balance for our staff. We believe that by doing this, staff wellbeing is enhanced and they are generally better placed to meet the needs of pupils. Some staff express a preference to undertake work from home. This is generally discouraged in pursuit of a work life balance. Therefore, school staff should undertake most school work when on site.

Mobile devices have the potential to make working practices more efficient to achieve a better work life balance. However, using these devices also creates additional risk for data security. This policy is designed to give the school's position on working from home.

Paper Based Data Security

Output paper based which contains Sensitive/protected information should not be taken off site under any circumstances.

In school, output Paper based information from ICT systems must be considered in light of its sensitivity as personal or confidential in nature. RESTRICTED information should have appropriate controls in place to protect it. A risk assessment should identify the appropriate level of protection for the information being stored. Sensitive information on printed paper on desks or in an open office must be protected by the controls for the building and other appropriate measures that could include:

- Filing cabinets or desk drawers that are locked with the keys stored away from the source.
- Locked safes
- Stored in a Secure Area protected by access controls.

Mobile Technologies

There are a range of mobile devices in operation across the school. These include:

- Encrytped Memory sticks
- Encrypted laptop computers
- iPad's
- IT Suite

Personal/sensitive information should only be stored on school owned, encrypted devices. In addition, personal/sensitive information should only be stored on a school owned device if absolutely necessary to do so and should be time limited. Personal/sensitive information should only be stored in the long term on the school's servers. Personal/sensitive information should not be stored on any personal device.

Appendix 3 Staff / Governors Acceptable Use Agreement:

Staff consent agreement for use of personal data:

Dear Staff Member,

At Ysgol Bryn Castell (YBC), we would like to seek your consent for some of the ways we take and use your photo.

Using your photo helps us to show members of the school community who works here.

We would like your consent in order to take and use your photo in the ways described below. If you're not happy for us to do this, that's no problem – we will accommodate your preferences.

Please tick the relevant box(es) below, sign and return this form to school.

Use of personal data	Tick (√)
I give permission for the school to use my photo in **displays in school**.	
I give permission for the school to use my photo on the **school website**.	
I give permission for the school to use my photo in the **school newsletter**.	
I give permission for the school to use my photo in **social media**.	
I give permission for the school to share my photo for **use in the media**	
I give permission for the school to **film me teaching**.	
I do NOT give permission for the school to use my personal data for any of the above purposes.	

If you change your mind at any time, you can let us know by emailing admin@ybc.bridgend.cymru, calling the school on 01656 815595, or just popping in to the school office.

If you have any other questions, please get in touch.

Why are we asking for your consent?
You may be aware that new data protection rules came into effect 25th May 2018. To ensure we are meeting the new requirements, we need to seek your consent for some of the ways we use information about you.

We would appreciate you taking the time to give consent again, as we really value being able to use the information in the ways listed above.

Staff member's signature: _____

Date:

Governors Agreement:

Dear School Governor,

At Ysgol Bryn Castell (YBC), we would like to seek your consent for some of the ways we use your information.

- We would like to take and use your photo. This will be used on the school website and other official school documentation which helps us to give members of the school community more of a sense of who our governors are
- To help you stay in the loop with what's going on in school, we would like to send you our newsletter, and emails about school events including fundraising to continue to improve the experience of the pupils at YBC
- Let you know about events and information which are specific to your role as School Governor

We would like your consent in order to do this, and use the information in the ways described above. If you're not happy for us to do this, that's no problem – we will accommodate your preferences.

Please tick the relevant box(es) below, sign and return this form to school.

Use of personal data	Tick (√)
I give permission for the school to use my photo in displays in school.	
I give permission for the school to use my photo on the school website.	
I give permission for the school to send me the school newsletter.	
I give permission for the school to email me about events in school.	
I give permission for the school to contact me on behalf of the Friends of YBC about its activities.	
I give permission for the school to use my contact details to contact me about fundraising activities.	
I give permission for the school to contact me on behalf of external providers and stakeholders about events specific to my role as a School Governor.	
I do NOT give permission for the school to use my personal data for any of the above purposes	

If you change your mind at any time, you can let us know by emailing admin@ybc.bridgend.cymru, calling the school on 01656 815595, or just popping in to the school office.

If you have any other questions, please get in touch.

Why are we asking for your consent?
You may be aware that new data protection rules came into effect from 25th May 2018. To ensure we are meeting the new requirements, we need to seek your consent for some of the ways we use information about you.

We would appreciate you taking the time to give consent again, as we really value being able to use the information in the ways listed above.

Governor's name: _____

Governor’s signature: _____

Date: _____

Appendix 4 - Privacy Notice (Parents, Carers, Pupils)

Consent Forms:

Dear Parents and Carers

At Ysgol Bryn Castell (YBC), we use information about you and your child in a number of different ways, and we would like your consent for some of the ways we use this personal data. We set these out in more detail below.

If you're not happy for us to use information in the ways we list below, that's no problem – we will accommodate your preferences.

Similarly, if you change your mind at any time, you can let us know by emailing admin@ybc.bridgend.cymru, calling the school on 01656 815595, or just popping in to the school office.

If you have any other questions, please get in touch.

Why are we asking for your consent again?
You may be aware that new data protection rules started on 25th May 2018. To ensure we are meeting the new requirements, we need to re-seek your consent for some of the ways we use information about you. There is a privacy notice displayed on the school website which explains the data YBC hold and the reasons why this is held by the school.

We would appreciate you taking the time to give consent again, as we really value being able to use the information in the ways listed below.

Photos and videos
We sometimes take photographs of pupils. We use these photos to help us to give people an idea of what life at our school is like, for example in the newsletter and on the school website.

Please tick the relevant box(es) below, sign and return this form to school.

Use of photos	Tick (√)
I give permission for the school to take photos of my child.	
I give permission for photos of my child to be used on the school website.	
I give permission for photos of my child to be used in the school newsletter.	
I give permission for photos of my child to be used in printed school materials, for example, the school prospectus.	
I give permission for photos of my child to be used in internal displays.	
I give permission for photos of my child to be used in the media, for example local newspapers.	
I give permission for photos of my child to be used on social media, for example Twitter.	
I give permission for the school to take videos of my child.	

I give permission for the school to use videos of my child for promotional purposes, such as on the school website.	
I do NOT give permission for the school to take or use photos of my child.	

Medical information

We would like your consent for some of the ways we store and share medical information about your child.

We would like to:

- Share information about your child with health professionals coming in to school, for example to do vaccinations and eye tests
- Take information such as height and weight for public health monitoring initiatives

This makes it easier for us all to keep your child healthy.

Use of information for medical purposes	Tick (√)
I give permission for the school to share information such as my child's height and weight with the NHS.	
I give permission for the school to share information such as my child's height and weight with the local authority.	
I give permission for the school to share information about my child (e.g., name) with health professionals doing vaccinations.	
I give permission for the school to share information about my child (e.g., name) with health professionals doing vision checks.	
I give permission for the school to share information about my child (e.g., name) with educational psychologists.	
I do NOT give permission for the school to use and share medical information in these ways.	

YBC would also like to seek your consent for some of the ways we use your information.

We will contact you using your:

- Home and mobile phone numbers (including by text message)
- Work phone number in emergencies (if applicable)
- Email address
- Postal address

Using your contact details in these ways helps us to:

- Keep you in the loop with what's happening at school including fund raising events
- Let you know about extra-curricular activities on offer for your child

If you're not happy for us to use information in the ways we list below, that's no problem – we will accommodate your preferences.

Similarly, if you change your mind at any time, you can let us know by emailing

admin@ybc.bridgend.cymru, calling the school on 01656 815595, or just popping in to the school office.

If you have any other questions, please get in touch.

Please tick the relevant box(es) below, sign and return this form to school.

Use of parents' contact details	Tick (√)
I give permission for the school to use my contact details to contact me about fundraising activities.	
I give permission for the school to use my contact details to contact me about the Friends of YBC fundraising activities.	
I give permission for the school to share my contact details with the Friends of YBC.	
I give permission for the school to use my email address to send me the school newsletter.	
I give permission for the school to contact me about clubs being run in school.	
I give permission for the school to contact me on behalf of external providers about events and clubs.	
I give permission for the school to share my contact details with health professionals doing vaccinations.	
I give permission for the school to share my contact details with health professionals doing vision checks.	
I give permission for the school to pass my details on to the secondary schools for which we are a 'feeder' school, so that they can contact me with information about their school.	
I give permission for the school to keep my child's contact details to contact them in the future about events including fundraising.	
I do NOT give permission for the school to use my personal data in the ways set out above.	

Your contact details

Name:

Home phone number:

Mobile phone number:

Work phone number:

Email address:

Postal address:

It is really important to update the School if any of your contact details change so that sensitive information is not send to an old postal or e-mail address or phone number.

Parent or Carer's signature: _____

Date:

Hwb Platform

In addition, schools have been asked by Welsh Government to gain consent to enable your son/daughter to use Hwb. Hwb is an online learning environment for School staff and learners which is managed by Welsh Government and every pupil in Wales will be given a secure log-in to the Hwb Platform.

From September 2018 onwards, Welsh Government will use Hwb to administer personalised online assessments which will replace the paper National Reading and Numeracy Tests. The Hwb Platform will also offer additional services to those pupils who have given their consent to receive them such as Hwb Classes, Microsoft Office 365, Google for Education, and other relevant educational tools and resources. These additional services are centrally funded and there is no cost for you or for your school to access and use them. We are therefore asking you to give consent for your son/daughter to access those additional services by signing and returning the attached form.

Consent form; The Hwb platform

The Hwb platform provides all maintained schools in Wales with access to a wide range of centrally-funded, bilingual digital tools and resources to support the digital transformation of classroom practices. The Hwb platform is managed and operated by the Welsh Government.

All pupils in maintained schools in Wales must be provided with a secure log-in to the Hwb platform. This is because mandatory reading and numeracy tests, currently on paper, will be moving online and must be completed by each pupil via the platform. In order to provide your child with a secure log-in, the school will be sending basic information to the Welsh Government. The log-in will allow your child to take the mandatory online assessments, known as 'personalised assessments'.

For more information about the Hwb platform and how information about your child is used, please see https://hwb.gov.wales/privacy .

For more information about the online personalised assessments, please see:

Personalised assessments: information for parents and carers - Hwb (gov.wales)

Additional services

If you agree, Welsh Government can also provide your child with access, via the Hwb platform, to a variety of additional services which are provided by other organisations. These include online learning environments such as Hwb Classes, Microsoft Office 365, Google for Education, and other relevant educational tools and resources. Welsh Government is making these additional services available to help you access educational resources. These additional services are centrally funded and there is no cost for you or for your school to access and use them.

Welsh Government will only provide access to these additional services if you sign the form below to indicate your agreement.

Your agreement

If you agree:

- we will tell Welsh Government to provide access to the additional services

- Welsh Government will share information about your child with its service provides, including Microsoft and Google Education, in order to enable access to the additional services

If you do not agree, we will still share information about your child with Welsh Government to set up a secure log-in for the Hwb platform, but your child will not be able to access the additional services.

If you wish to withdraw your consent, please contact the head teacher within your child's school.

Please sign and date this form if you agree to the above.

Signed .....

Name .....

Date .....