Ysgol Pen-y-Bryn
Data Protection & Access to Records Policy

As a Rights Respecting School, we are committed to embedding the principles and values of the United Nation Conventions for 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 28 – Every child has the right to an education.
Article 29 – Education must develop every child's personality, talents and abilities to the full.
Article 42 – Every child has the right to know their rights.

Headteacher…… Date …17/2/22……

Chair of Governors …… Date …17/2/22……

Review Date …17/2/23……

Contents

Appendices

(i) Introduction

Ysgol Pen-y-Bryn collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations. This policy should be read in conjunction with the School privacy notice which is published on the school website (Appendix 1).

(ii) Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulations (the GDPR), the Data Protection Act 2018, and other related legislation. This policy 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. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

The school is committed to maintaining the data protection rights and principles at all times.

Therefore the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary and to comply with the Welsh Guidance in Circular 18/2006 regarding the transfer of pupil information to any new school and in accordance with the school retention guidelines (appendix iv).
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely.
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded

- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information
- Ensure our staff are aware of and understand our policies and procedures

(iii) Data Protection Definitions

'personal data' - any information relating to an identified or identifiable natural person *('data subject')*; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'sensitive personal data' (AKA Special Categories of Data) - data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

'processing' - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'controller' - the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

'processor' - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

'consent' of the data subject - any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

'personal data breach' - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(iv) Data Protection Principles

The school staff shall at all times comply with the following GDPR data protection principles:

1. *Lawfulness, fairness and transparency* - Personal data can only be processed if there is a lawful basis for doing so. It must be fair to the data subject and you must be fully transparent with the data subject as to why you are collecting their data and how it is going to be used and shared.
2. *Purpose Limitation* - Data should only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, although further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is permitted in certain circumstances.
3. *Data Minimisation* - Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
4. *Accuracy* - Personal data must be accurate and, where necessary, kept up to date. Where personal data is inaccurate every reasonable step should be taken to enable its deletion (where appropriate) or correction without delay.
5. *Storage Limitation* - Personal data must be kept in a form that permits the identification of data subjects for no longer than is necessary. Such personal data can be stored for longer periods for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in certain circumstances and subject to the implementation of the appropriate technical and organisational measures.
6. *Integrity and Confidentiality* - Personal data must be processed in an appropriately secure manner including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by the use of appropriate technical or organisational measures.

(v) Data Subject Rights

Some of the rights below are subject to restrictions, however staff should be aware of these rights and should endeavour as far as possible and in consultation with the Headteacher to further the following rights:

1. *The right to be informed* - Data controllers must be completely transparent with data subjects about the processing of their data by

providing information in a 'concise, transparent, intelligible and easily accessible form, using clear and plain language'.
2. *Right of Access* - Data subjects have the right of access to their records 'without undue delay and within one month of the request'. An extension of a further two months is permissible in certain circumstances. See attached appendix 1 for detail of the operation of this right in practice.
3. *Right to Rectification* - The data subject has the right to obtain from the data controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purpose of the processing, the data subject also has the right to have incomplete personal data completed including by means of providing a supplementary statement.
4. *Right to Restrict Processing* - The data subject can ask for there to be a restriction on processing such as where the accuracy of the personal data is contested. This means that the data controller may only store the personal data and not further process it except in limited circumstances.
5. *Right to Object* - Data subjects can object to certain types of data subject does not need to show grounds for objecting).
6. *Rights on Automated Decision Making and Profiling* - The GDPR provides safeguards for data subjects against the risk that a potentially damaging decision is taken without any human intervention.

(VI) Complaints (Data Handling) and Reviews (Subject Access Requests)

It is important to recognise the correct procedure for dealing with a grievance that may be raised.
Complaints about data handling will be dealt with in accordance with the school's Complaints Policy. The school's Complaints Policy does not apply to expressions of dissatisfaction about information requests such as a Subject Access Request response, a response to a request for an Educational Record or a Freedom of Information response, which instead will be subject to a process of internal review. The internal review will be undertaken by the Chair of Governors and the Headship Team.

e.g. Parent A is unhappy that their information was inadvertently disclosed to a third party without their permission. This is a complaint about data handling and is capable of being investigated under the school complaints policy.

Parent B has made a subject access request for all of his child's records. Exemptions have been applied and some records have been withheld to protect the child from harm. Parent B is unhappy with the outcome that records were withheld. This is a complaint about the outcome of an information request and would be subject to internal review rather than the school complaints procedures.

Parent C is dissatisfied that a request to amend the child's record to include them as a key contact has not taken place. This is a complaint about data handling and can be subject to the complaints procedures.

Parent D submits a Freedom of Information Request for the number of pupils excluded for possession of a knife. The school refuse the request as only 1 pupil has been excluded and to respond would inadvertently identify the pupil and the reason for the exclusion. The parent can request an internal review as this is an information request.

Any complaints – whatever the issue (data handling or information requests) can be referred for investigation to the independent supervisory authority – The Information Commissioner. The Information Commissioner usually requests that expressions of dissatisfaction are dealt with at local level before they will investigate but data subjects are free to lodge complaints with the Information Commissioner at any time. Information Commissioner's Office – Wales 2nd Floor, Churchill House Churchill Way Cardiff CF10 2HH Telephone: 029 2067 8400 Fax: 029 2067 8399 Email: wales@ico.org.uk

(vii) Data Protection Impact Assessments

A Data Protection Impact Assessment [DPIA] is a tool designed to: -

- Describe the data processing activity undertaken or proposed
- Assess whether the processing activity is necessary and proportionate
- Identify and plan mitigation for any risks associated with the processing activity

The completion of a DPIA is mandatory in certain circumstances and a failure to carry out a DPIA would mean that the School is failing in its legal obligations. Below are the four considerations that should lead staff to consider the completion of a DPIA.

1. Commencing or designing a new project / activity that would involve the processing of personal data. E.g. deciding to install a new CCTV camera.
2. Utilising a new technology or system for processing or holding personal data.
   E.g. ending the contract with the current software supplier and moving to a new software system in a department.
   E.g. wearable body cams were a relatively new technology that raised particular privacy issues when first introduced a few years ago. Fingerprint and facial recognition are other examples of new technologies.
3. An existing method of processing personal data has proven ineffective or is at risk of exposing personal data to unauthorised access, disclosure, alteration and / or deletion.
   E.g. a data breach highlights that the safeguards in place for the processing activity are insufficient whether that be as a result of human error, process flaw or technological weakness
   E.g. a cyber-attack of another organisation reveals a flaw in a particular operating system that is also utilised by this School.
4. An existing processing operation has altered significantly since its implementation.
   E.g. where a new technology is used for the processing operation or because the personal data is being used for a different purpose than originally designed.

The school will adhere to the guidance and utilise the DPIA Screening forms issued by Swansea Council as available on Staffnet.
http://www.swansea.gov.uk/staffnet/DPIA

The data protection officer for the school however retains autonomy to decide whether a DPIA should be completed and the form of the assessment.

(viii) Data Breach Procedures

'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

These procedures apply to all staff within the school. If any user is found to have seriously breached this policy, they may be subject to disciplinary

procedures. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s).

A data breach includes, but is not restricted to, the following:-

- Disclosing personal information to someone not authorised to have it; verbally, in writing or electronically.
- Unauthorised access to information via a software application;
- Uploading personal information to a website in error;
- Human error resulting in personal information being left in an insecure location;
- Providing data via an email scam
- Finding data that has been changed by an unauthorised person.
- Printing or copying confidential information and not storing it correctly or confidentially.

The School recognises that there are risks associated with users accessing and handling data in order to conduct official School business.

This policy aims to mitigate the following risks:-

- To reduce the impact of data breaches by ensuring incidents are followed up quickly and effectively.
- To help identify areas for improvement to decrease the risk and impact of future incidents.

Non-compliance with this policy could have a significant effect on the effective operation of the School and may result in financial loss as a result of fines levied. **Data breaches must be reported to a member of the senior Leadership Team at the earliest possible stage so they can be assessed and investigated.**

The Investigation Stages

Part 1 Breach Form (Appendix iv)

1. Staff member reports possible breach to the head teacher who will either investigate or appoint an investigating officer (IO) as soon as the breach is discovered.
2. The IO initially evaluates the risk to the rights and freedoms of individuals involved in the breach and will immediately work towards containment and recovery of the data. Containment and recovery must not be delayed.

3. The IO will consider whether to contact the data subject (if high risk) to ensure they are aware of the breach and for them to take any necessary actions to mitigate any further risks. High risk would include circumstances where for example financial data has been misplaced and the data subject will need to take urgent action with their bank to prevent any fraud.
4. IO completes part 1 of the breach report within 24 hours and will circulate to the lead governor for data protection, the Headteacher (if not acting as the IO) and the school Data Protection Officer.

The Breach Panel – Part 2 Breach Form

5. A breach panel consisting of the persons noted at point 4 will be set up to complete part 2 of the breach form and to decide if the matter should be referred to the ICO. The panel will also decide whether to inform the data subject if they have not been made aware at point 3.

NOTE: Points 1-5 need to be undertaken within the first 72 hours of identifying the breach. Should you need to refer a matter to the ICO and 72 hours has expired you will need to explain why it was not possible to comply with the 72 hour timescale.

6. Breach panel will discuss the breach and provide recommendations.

Follow Up – Part 3 Breach Form

7. IO ensures all recommendations from the breach panel are implemented and will meet with the Governor in charge of Data Protection to provide evidence of this.
8. Part 3 of the breach form shall be updated with all actions undertaken and the completed breach form held in a central data breach file.

(ix) Other Relevant Policies -

The following school policies are of relevance:

- ICT Policy,
- Use of Internet & ICT Systems
- E-Safety – Pupil Acceptable Use Policy
- Staff Disciplinary Policy

(x) Staff Training

To ensure that all staff are aware of their responsibilities regarding the safe handling of personal data it will be mandatory for all staff to undertake training. The school will utilise the e-learning modules available from Swansea Council and any other training materials thought appropriate to ensure staff have the necessary skills to understand the importance of adhering to the data protection principles.

All staff at induction will be required to complete the e-learning module regarding information security and management. Training records will be maintained to ensure refresher data protection training is undertaken by all staff at intervals of no less than once every three years. Governors will also undertake this training.

(xi) Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than once every two years.

Appendix 1 – Pen-y-Bryn Privacy Notice

Ysgol Pen-y-Bryn Privacy Notice

Identity and contact details

Our postal address is: Ysgol Pen-y-Bryn, Glasbury Road, Morriston, Swansea, SA6 7PA

Our website address is: www.ysgolpenybryn.co.uk

Issues of how data is handled are dealt with by the Headteacher or the School's Data Protection Officer.

As a public authority, we must comply with all relevant legislation relating to data handling. The Information Commissioner's Office (ICO) is the supervisory authority in the United Kingdom established to ensure that your data rights are upheld.

Categories of personal data we hold

Obtaining, recording, holding and dealing with personal information is known as 'processing'.

As a school the vast majority of information we collect is about our pupils but we do also hold key information needed about parents / guardians and staff members.

Generally a school file may include:-

- Attendance data
- Academic achievements and progress
- Ethnicity

- Wellbeing and pertinent health information (medication, allergies and illnesses)
- Free School Meal eligibility
- Contact details of parents and guardians
- Minutes of meetings relating to the child
- Statement of Special Educational Need and reviews of the same
- Reports and referrals to and from other agencies if applicable – Youth Offending Service and Social Services for example

The school as an employer will also hold a personnel file for all staff and this file will generally consist of:-

- Contact details
- Bank details, National Insurance Number for payroll purposes
- Details of any references or DBS checks where applicable
- Details of driving licence and vehicle MOT / Insurance
- Details of any disciplinary action
- Information regarding sickness and annual leave

How the School collects and uses personal data

The School has a responsibility to provide its pupils with a good education in a safe environment. It is necessary to collect personal data to enable the school to provide pupils with an education, to track and monitor academic progress and to ensure those with parental responsibility are kept informed of key milestones and achievements.

Some of the information will be provided to us by parents / guardians and some will be generated by us whilst the pupil is in our School.

Here are some examples of how we collect and use your data:

Providing an education:

We generate and then hold the reports of a pupil's progress and any examination results. We generate and keep attendance data which can be analysed to ensure that children are attending school regularly and attending on time. The school will on occasion utilise educational apps and websites with the children, all of which will be undertaken under the supervision of a staff member.

Maintaining school discipline and awarding positive behaviour:

As part of the school file we will create a behaviour record that would include all significant incidents of breaches of the school discipline policy. This would include any fixed term or permanent exclusions. The school file will also include examples of excellence and achievements.

Keeping learners safe and improving wellbeing:

There may be occasion when the school will collect documentation regarding the wellbeing of pupils. It is a legal requirement for all schools to develop and have in place systems of safeguarding and promoting the wellbeing of children in their care. This may involve documenting concerns and receiving information from other agencies such as social services when they have a worry about a pupil. Monitoring wellbeing allows the school to ensure the best possible services and support are available to the pupil and their families.

Keeping parents updated and involved in the school:

We do collect details of parents and guardians to ensure that we are able to keep you informed of school events and activities.

Recruitment:

When individuals apply to work for the School, we will only use the information they supply to process their application and to monitor equal opportunities statistics. Personal information about unsuccessful candidates will be held for six months after the recruitment process has been completed, it will then be destroyed securely.

Once a person has taken up employment with the School we compile a personnel file relating to their employment. The information contained in this is kept secure and will only be used for purposes directly relevant to that employment.

The Source of Personal Data

The vast majority of personal data we hold will have been generated in the course of a pupil attending the school or will have been provided to us

directly from you. There are occasions where personal data is collected about you in other ways.

This includes:

- When partner agencies share information with us to provide a joined-up service to you.

- When you move into our local authority area, data may be shared from the previous school or local authority area.

People We Share Data With

Service Provision:
We may share data with others to enable a requested or statutory service to be provided. This could be where we use another agency to deliver the service for us or where we collaborate with other agencies. An example would be that information would be shared with the Local Authority to enable an assessment of a child's special educational needs. Another example would be the supply of information at your request to contribute to a Child and Adolescent Mental Health assessment.

Transfer of information to another school / local authority:
Personal information about you may also be provided to other local authorities or schools. An example would be where you have moved from one area to another or start at a new school. The school file will be securely transferred to the new Local Authority / School.

Health Information
In some circumstances we may share information with NHS professionals providing services to our school children. This would be for services such as vaccinations, dental provision and school nursing activities.

We may collect health information on staff members when such information is supplied as part of the sickness policy and / or following referrals to occupational health.

Transfer of information required by law:
We also share personal information where we are required to do so by law. Examples include where we are required by law to report matters to

Welsh Government who then in turn publish a lot of the data they receive:
https://statswales.gov.wales/catalogue/education-and-skills

Another example would be our duties to share information with social services when they are carrying out their protective functions or the police when carrying out investigations.

How long we keep your data

Data is held for no longer than is necessary and the School follows legal guidelines on how long information should be kept before it is securely destroyed.

The timeframe for holding data is different depending on the type of data involved.

To see our full retention schedule please visit our website where the retention schedule is included in our Data Protection Policy.

Transfers outside the European Economic Area

We do not share personal information beyond the European Economic Area (EEA) save for should a pupil move to a school outside of the EEA. This is quite rare but does occur particularly with children of British Forces personnel. In this circumstance the school file will be securely transmitted to the new school / authority as appropriate.

Your Data Rights

In so far as is compatible with legal requirements you have a number of rights in respect of your data:

1. **Right to be informed**. We must be completely transparent with you by providing information 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language'. Our privacy notice is one of the ways we try and let you know how data is handled.

2. **Right of access**. You have the right to access your personal information. Parents also have the right to access the educational record of the pupil.

3. **Right to rectification**: You have the right without undue delay to request the rectification or updating of inaccurate personal data.

4. **Right to restrict processing**: You can ask for there to be a restriction of processing such as where the accuracy of the personal data is contested. This means that we may only store the personal data and not further process it except in limited circumstances

5. **Right to object**: You can object to certain types of processing such as direct marketing. The right to object also applies to other types of processing such as processing for scientific, historical research or statistical purposes (although processing may still be carried out for reasons of public interest).

6. **Rights on automated decision making and profiling**: The law provides safeguards for you against the risk that a potentially damaging decision is taken without human intervention. The right does not apply in certain circumstances such as where you give your explicit consent.

7. **Right to data portability:** where personal data is processed on the basis of consent and by automated means, you have the right to have your personal data transmitted directly from one data controller to another where this is technically possible.

8. **Right to erasure or 'right to be forgotten'**: you can request the erasure of personal data including when: (i) the personal data is no longer necessary in relation to the purposes for which they were collected (ii) you no longer provide your consent, or (iii) you object to the processing.

The Information Commissioner regulates data handling by organisations in the U.K. and work to uphold the data rights of citizens, their website provides more information on the rights available to you:

https://ico.org.uk/for-the-public/

Withdrawing Consent

If you consented to providing your personal information to us and you have changed your mind and you no longer want the School to hold and process your information, please let us know.

If you encounter any difficulties in withdrawing consent, please contact the School Data Protection Officer or the Headteacher.

Automated Decision Making and Profiling

The School does not carry out automated decision-making, and as such any decision taken by us which affects you will always include human intervention. We do on occasion carry out profiling and track the progress of pupils to enable us as a School to target services to those who are in need of help and support.

The Right to Complain About Data Handling

The School sets very high standards for the collection and appropriate use of personal data. We therefore take any complaints about data handling very seriously. We encourage you to bring to our attention where the use of data is unfair, misleading or inappropriate and we also welcome suggestions for improvement.

Informal Resolution:
In the first instance we would ask that you try and resolve data handling issues directly with the Headteacher or any member of the senior leadership team. We are committed to handling data appropriately and are confident that we can resolve most issues informally.

Formal Resolution:

You can ask for your issue to be investigated by writing to:

If you remain dissatisfied following the response to your contact with the school, if it relates to issues of data handling you can raise the issue with the Information Commissioner. It is free of charge to contact the Information Commissioner and request their assistance.

Information Commissioner's Office – Wales
2nd Floor, Churchill House
Churchill Way
Cardiff
CF10 2HH

Telephone: 029 2067 8400
Fax: 029 2067 8399
Email: wales@ico.org.uk

Appendix 2 - Guide to Information Requests

Procedures for responding to Requests for Personal Information

This guide is not to be read in isolation when dealing with a request for information. When processing a request for information the web resources listed in appendix 6 should also be considered.

Rights of access to information

There are two distinct rights of access to information held by schools about pupils.

1. A subject access request (SAR) - Under the Data Protection Act any individual has the right to make a request to access the personal information held about them.
2. A request for an 'Educational Record' - The right of those with parental responsibility entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

Is the request a Subject Access Request or a request for an Educational Record – What is the difference?

As different time limits, fees and type of record capable for disclosure apply depending on the type of request, it is important to understand what the request is for. It is likely that it will not be evidently clear whether the request is a SAR or request for an Education Record and it is also likely the request may be a bit of both.

Quite often the person making the request will not know the difference between a request made under the Data Protection Act and the Pupil Information (Wales) Regulations and therefore the school may need to clarify and where appropriate assist the individual understand the difference and make the request that best suits their needs.

SAR – a subject access request is the right of an individual to access any information held by the school about themselves. In relation to children, a person with parental responsibility is able to make this request on

behalf of their child if the child is not of sufficient age and understanding to do so themselves.
A subject access request is more likely to be worded in terms such as:- 'I want to have access to all information held about my son'
A request for a copy of the 'Educational Record' maybe more in terms of:- 'I want all updates in relation to my daughters progress'.
It is a subtle difference but an important one.

An education record consists of:-

1. Curricular record: a formal record of a pupil's academic achievements, other skills and abilities and progress within school
2. Teachers record: any record kept by the teacher at the school that is not intended to be kept solely for that teachers own use.
3. Any other educational record relating to the pupil in addition to the curricular record.

Both a request for an Education Record and a Subject Access Request are subject to exemptions. This policy should be read in conjunction with the ICO Guide to Subject Access which sets out the procedure and exemptions.

If an exemption applies the school should consider carefully in accordance with the ICO guidance whether to release the information at all or in a redacted format.

A common example of where it might be appropriate to apply an exemption and to withhold information would include:-
- Information that might cause serious harm to the physical or mental health of the pupil or another individual;
- Information that might reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests;
- Information contained in adoption and parental order records; and
- Certain information given to a Court in proceedings concerning the child.
- Management / forecasting information generated for example during a redundancy situation would be exempt from subject access.

If the record contains information about other children or 3rd parties consider whether or not that information should be removed. Particularly where it is personal information relating to the 3rd party and it is sensitive in nature.

The right of access only extends to data belonging to that individual and not to data about anyone else.

Actioning a request for Information

1. Requests for information must be made in writing; which includes email, and be addressed to the School Data Protection Officer. If the initial request does not clearly identify the information required, then further enquiries will be made. Consider whether this is a Subject Access Request or a request for the Educational Record.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:
   - passport
   - driving licence
   - utility bills with the current address
   - Birth / Marriage certificate
   - P45/P60
   - Credit Card or Mortgage statement

3. For subject access requests any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher or appropriate person should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The school may make a charge for the provision of information, dependent upon the following:
   - Should the information requested contain in whole or part the educational record then the amount charged will be dependent upon the number of pages provided.
   - Should the information requested be personal information that does not include the Educational Record the school cannot charge a fee to provide it.

5. The response time for subject access requests, once officially received, is 1 month which can in certain circumstances be extended by a further period of 2 months.

NOTE HOWEVER THAT IF THE SAR INCLUDES IN WHOLE OR PART A REQUEST FOR A PUPIL'S EDUCATION RECORD A RESPONSE MUST BE PROVIDED IN 15 SCHOOL DAYS.

6. The Data Protection Act allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure. The professional considering disclosure must look at whether the information should be withheld in accordance with any exemption.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to timescales. Consent or otherwise is not determinative of whether you release information. See the Subject Access Code of Practice for the balancing exercise to be undertaken.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought. The schools benefit from a Service Level Agreement with the legal department of the City and County of Swansea and the school is encouraged to make contact and discuss requests.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why. Care should be taken with redaction to ensure if sensitive information is removed it cannot be seen. This may involve

photocopying the material after redaction to ensure that the information cannot be seen.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Appendix 3 – School Arrangements for Data Protection

To maintain appropriate arrangements for Data Protection it is necessary to define and outline the roles and responsibilities within the school.

Governing Body - As the 'data controllers' for the school's data the Governing Body are ultimately responsible for all data processing arrangements within the school. They shall ensure that a review of the data protection policy takes place at no less than once every two years.

Lead Governor for Data Protection - The lead governor will have the necessary skills and abilities to understand the processing activities of the school and be able to work to improve data protection practice within the school. They will be an invitee to any data breach panel organised.

Headteacher - The Headteacher has delegated responsibility from the Governing Body to act on their behalf and ensure staff comply with policies and procedure. The Headteacher will oversee and will facilitate themselves or via other staff members records requests from pupils and parents.
The Headteacher will either conduct themselves or will delegate to an appropriate staff member the following:-
- The role of investigating officer if a data breach occurs
- The completion of a Data Protection Impact screening / full form if required.
The Headteacher (along with any investigating officer) will be an invitee to any breach panel.

All Staff Members - All staff members must ensure that they handle data safely and to not place the personal data of pupils or parents at risk of unauthorised access, loss or deletion. All staff members should highlight any areas of concern regarding data handling so that practice can be improved within the school and ensure the data protection principles are adhered to.

Data Protection Officer [DPO] - The DPO will be responsible for providing advice and assistance to all staff in relation to the schools current and proposed processing activities. The DPO in providing advice and assistance will be endeavouring to create a culture of data protection.

The DPO must be consulted whenever a Data Protection Impact Assessment is contemplated. The DPO has autonomy to insist that an assessment takes place. The DPO will have a good knowledge of data protection and will be afforded the time to train and develop their understanding. The DPO will be responsible for ensuring that the Register of Processing Activities for the school is maintained and up to date. The DPO will challenge and ensure that the mandatory induction and refresher training of all staff is completed and accurate staff training records are held by the school. The DPO will be the first point of contact for the Information Commissioner should there be a complaint, data breach or other matter being dealt with directly by the supervisory body. The DPO cannot be a person who has a role that conflicts with their day to day role. The DPO cannot be asked to decide what personal data to collect, how and why as part of their job role. The DPO must have the ability to be independent and challenge data handling and as such cannot be an individual who:- - Decides on the mode or method of processing - Decides which system(s) to procure or utilise - Provides technical management of ICT systems - Is the lead staff member for an area that has responsibilities for data handling It may therefore not be appropriate for the DPO to be the head teacher, systems manager / head of ICT or lead safeguarding officer.

Appendix 4 – Data Breach Form

Part 1 – Description of Breach

Investigating Officer	
Role	
Date form completed	
Date and time breach was discovered. Explain any significant delay in compiling this report.	
Describe the breach, explaining the cause, the staff members involved and indicating how widely the data was disclosed.	
How many people (data subjects) are affected by the breach?	
Will the breach create a risk to the freedoms of the data subject(s), namely discrimination of any kind, identity theft, reputational or financial loss?	
Detail your response to the breach so far, including any efforts made to recover the data and to mitigate any possible adverse effects to the data subject(s)	

Part 2 – Data Breach Panel Overview

Date of committee meeting	
Attendees	
Has the panel met within 72 hours of the data breach being discovered? If not explain reasons for delay.	
Summary of any further evidence presented to the panel by the Investigating Officer.	
Decision to refer breach to ICO or no, including justification	
Decision to inform data subject of breach (if not already done so) including rationale. (The Panel must consult with the Council's Data Protection Officer (DPO) to confirm any decision not to inform the data subjects of the breach.)	
Summary of panel recommendations to improve practice.	

Part 3 – Follow Up

Date of meeting between reviewing officer and Governor in charge of data protection.	
Evidence shown to ensure recommendations have been met	

Appendix 5 – Retention Schedule

The school shall comply with national guidelines on retention of information supplied by the Information and Records Management Society.

Further details on this can be requested from the school or the following link

http://ldbsact.org/download/policies/Document%20Retention%20Schedule_Nov15.pdf

Appendix 6 – Useful Links

Data Breaches –

https://ico.org.uk/media/fororganisations/documents/1562/guidance_on_data_security_breach_management.pdf

Data Protection Guidance –

https://ico.org.uk/for-organisations/education/

https://www.swansea.gov.uk/GDPRchanges