Penyrheol Comprehensive School

Data Protection and Access to Records Policy

Date Adopted	**May 2018**
Last Reviewed	**June 2019**
Date for Next Review	**June 2020**

Contents

Appendices

Introduction and the UNCRC

Penyrheol Comprehensive School 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.

This policy supports the United Nations Convention on the Rights of the Child, the most complete statement of children's rights ever produced. This is in particular in relation to the following articles:

Article 3 (best interests of the child)
The best interests of the child must be a top priority in all decisions and actions that affect children.

Article 8 (protection and preservation of identity)
Every child has the right to an identity. Governments must respect and protect that right, and prevent the child's name, nationality or family relationships from being changed unlawfully.

Article 12 (respect for the views of the child)
Every child has the right to express their views, feelings and wishes in all matters affecting them, and to have their views considered and taken seriously.

Article 28 (right to education)
Every child has the right to an education. Primary education must be free and different forms of secondary education must be available to every child. Discipline in schools must respect children's dignity and their rights.

Purpose of the Policy

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 4).
- Ensure that when obsolete information is destroyed 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.

Key Data Protection Definitions

‘personal data’ means 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) means 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’ means 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’ means 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’ means 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 means 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’ 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.

Data Protection Principles

The school staff shall at all times comply with the following 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.

Overarching Duty of Accountability

The data controller should keep records evidencing its compliance with the above principles. Such record keeping would include the logging of any new system or processing activity onto the Register of Processing Activities.

For more information visit:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Summary of 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. 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 processing such as direct marketing (which is an absolute right for which the 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.

Complaints [data handling] vs Reviews [information 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, which is published on the school website.

However, the school 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 a member of the senior leadership team.

For example, 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 certain 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 Policy.

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 Policy.

Parent D submits a Freedom of Information Request for the number of pupils excluded for possession of a knife. The school refuses 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 Office 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

Data Protection Impact Assessments [DPIA]

A 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 examples of considerations that should lead staff to complete a DPIA:

Commencing or designing a new project / activity that would involve the processing of personal data.

E.g. deciding to install a new CCTV camera.

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.

E.g. fingerprint and facial recognition are other examples of new technologies.

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.

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 and Full Forms issued by Swansea Council:

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.

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 the Data Protection Officer or Headteacher at the **earliest possible stage** so they can be assessed and investigated.

The Investigation Stages – Part 1 Breach Form

1. Staff member reports possible breach to the Data Protection Officer or Headteacher 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 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.
8. The breach report shall be presented for the consideration of the Data [or other suitable] Committee for a review of actions taken.

9. 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.

Other Relevant Policies

The following Council and school policies are of relevance:

- Data Protection Privacy Notice
- Data Protection Accessing Records Policy
- Acceptable ICT Use Policy
- Mobile Phone Policy
- Safe Use of Images Policy.

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 two years.

Policy Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than once every three years. The policy review will be undertaken by the Headteacher, or nominated representative, in consultation with the school Data Protection Officer and the outcome of such a review shall be presented to the Governing Body for confirmation.

Appendix 1

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 5 should also be considered.

Rights of access to information

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

1. Under the Data Protection Act any individual has the right to make a request to access the personal information held about them. A Subject Access Request (SAR).

2. 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. A request for an 'Educational Record'.

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 to 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 SAR is more likely to be worded in terms such as:-
'I want to have access to <u>all information</u> 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 daughter's 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' records: any record kept by the teachers at the school that is not intended to be kept solely for an individual teacher's 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.
- 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 should be addressed to the school's 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

This list is not exhaustive.

3. For SARs, 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, dependant upon the following:

- Should the information requested contain <u>in whole or part the Educational Record</u> then the amount charged will be dependent upon the number of pages provided:

1 – 19	£1
20 – 29	£2
30 – 39	£3
40 – 49	£4
50 – 59	£5
60 – 69	£6
70 – 79	£7
80 – 89	£8
90 – 99	£9
100 – 149	£10
150 – 199	£15
200 – 249	£20
250 – 299	£25
300 – 349	£30
350 – 399	£35
400 – 449	£40
450 – 499	£45
500+	£50

- Should the information requested be personal information that does not include the Educational Record, the school cannot charge a fee to provide it.
- If the information requested is only the Educational Record, viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher in accordance with the schedule above.

5. The response time for SARs, once officially received, is one month, which can in certain circumstances be extended by a further period of two 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 2

School Governance 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 three years. At the time of policy review, the Governing Body shall receive updates from the lead governor for data protection, Headteacher, DPO, a representative of the Data Committee as to their work to improve data protection practice within the school.

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.

The Data Committee of the Governing Body

The Data Committee will develop a work plan for considering the data protection compliance within the school. The work plan will encompass but will not be limited to:

- Training of staff.
- Arranging periodical audits of school systems to ensure data is being held and processed safely.
- To consider whether any current ways of working can be improved so as to make data handling more secure.
- Scrutinise the proposed use of any new system.
- Discuss any data breaches that have occurred and overseeing the implementation of new procedures to prevent a repeated breach.
- The provision of communications to staff to raise awareness of data protection issues.

All Staff Members

All staff members must ensure that they handle data safely and do 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 school's 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 considered. 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 for whom the role would conflict 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 Headteacher, Network Manager, ICT Coordinator or lead Safeguarding Officer.

Appendix 3

Data Breach Form

Part 1 – Full description of the personal data breach

Name of Investigating Officer:		**Tel No.:**	
Department/Section/ Role:			
Date completed:		**Time completed:**	

1.1 Date and time the breach was discovered. Explain any significant delay in compiling this report.

1.2 Describe the breach, explaining the cause, the staff members involved and indicating how widely the data was disclosed.

1.3 List the categories of personal data (names, addresses, bank details etc) which were disclosed and if any classify as sensitive personal data? Sensitive personal data is 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

1.4 How many people (data subjects) are affected by the breach?

1.5 Will the breach create a risk to the rights and freedoms of the data subject(s), namely discrimination of any kind, fraud, identity theft, reputational or financial loss?

1.6 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 subjects.

1.7 Identify any reputational risks for the school or risks to public confidence.

Part 2 – Data Breach Panel overview

Date and time of panel:	
Attendees:	

2.1. Has the Panel met within 72 hours of the breach being discovered? If not, explain the reasons why there was a delay in convening the Panel

2.2. Summary of any further evidence presented to the Panel by the Investigating Officer

2.3. Record here the Panel's decision on whether to refer the breach to the ICO or not, with accompanying rationale.

2.4 Record here the Panel's decision on whether the data subject(s) should be informed of the breach or not, with accompanying rationale.

2.5. Summary of any recommendations for improving working procedures

2.6 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. If appropriate, record here the DPO's acceptance or otherwise of the Panel's decision on this, with any accompanying comments.

Part 3 – Post Implementation review

Date of Committee Meeting:	
Attendees:	

3.1. Overview of the breach and outcomes of the investigation. List the ways that the department responsible for the breach has since improved its practice.

3.2. Further recommendations, including the need for any further actions such as staff communications arising from the lessons learned.

Appendix 4

Retention Guidelines

Pupil Information

Basic File Description	Data Protection Issues	Statutory Provision	Retention Period	Action at end of administrative life of the record	Comment
Admission Register	Yes	None	Date of last entry in book (or file) + 6 years	Retain in the school for 6 years from the date of the last entry	Transfer to the archives
Attendance Registers	Yes	None	Date of register + 3 years	Destroy [if these records are retained electronically any back-up copies should be destroyed at the same time]	
Pupil record cards	Yes	None			
Secondary			DOB of the pupil + 25 years	Shred	
Pupil Files	Yes	None			
Secondary			DOB of the pupil + 25 years	Shred	
Special Educational Needs files, reviews and Individual Education Plans	Yes	None	DOB of the pupil + 25 years	Shred	
Letters authorising absence	No	None	Date of absence + 2 years	Shred	
Examination Results	Yes	None			
Public	No	None	Year of examinations + 6 years	Shred	Any certificates left unclaimed should be

					returned to the appropriate Examination Board
Internal examination results	Yes	None	Current year + 5 years	Destroy	
Any other records created in the course of contact with pupils	Yes / No		Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or destroy	

Basic File Description	Data Protection Issues	Statutory Provision	Retention Period	Action at end of administrative life of the record	Comment
Statement maintained under the Education Act 1996 s.324	Yes	SENDA 2001 SEN Code of Practice	DOB of the pupil + 30 years	Destroy unless legal action pending	The Additional Learning Needs and Education Tribunal (Wales) Bill and associated codes and regulations will provide the new statutory provision when in force.
Proposed Statement or amended Statement	Yes	SENDA 2001 SEN Code of Practice	DOB of the pupil + 30 years	Destroy unless legal action pending	The Additional Learning Needs and Education Tribunal (Wales) Bill and associated codes and regulations will provide the new statutory provision when in force.
Advice and information to parents regarding educational needs	Yes	SENDA 2001 SEN Code of Practice	Closure + 12 years	Destroy unless legal action pending	The Additional Learning Needs and Education Tribunal (Wales) Bill and associated codes and regulations will provide the new statutory provision when in force.
Children SEN Files	Yes		Closure + 35 years	Destroy unless legal action pending	

Management Information

Basic File Description	Data Protection Issues	Statutory Provision	Retention Period	Action at end of administrative life of the record	Comment
Records created by Headteachers, Deputy Headteachers, Heads of Year and other members of staff with administrative responsibility (except child protection records)	Yes	None	Closure of file + 6 years	Destroy. If the records contain sensitive information they should be shredded.	

Curriculum

Basic File Description	Data Protection Issues	Statutory Provision	Retention Period	Action at end of administrative life of the record	Comment
Examination Results	Yes	None	Current year + 6 years	Shred	

Child Protection

Basic File Description	Data Protection Issues	Statutory Provision	Retention Period	Action at end of administrative life of the record	Comment
Child Protection Records	Yes	Education Act 2002 s.172, Safeguarding Children in Education, All Wales Child Protection Procedures	DOB + 35 years*	Shred	Child protection information must be copied and sent under separate cover to new school/college whilst the child is still under 18 (i.e. the information does not need to be sent to a university for example). Where a child is removed from roll to be educated at home, the file should be copied to the local education authority.

* This retention period should be kept under review and take into account guidance issued from Welsh Government and/or the Independent Inquiry into Child Sexual Abuse [IICSA] as further guidance is issued and the inquiry progresses. The Independent Inquiry into Child Sexual Abuse (IISCA) has advised no records that meet the broad remit of the Inquiry should be deleted at all and should be retained. This D.o.b. +35 year policy is to be read in conjunction with guidance and recommendations issued as part of that Inquiry. The length of time set is reflective of seeking to achieve 3 key aims of: 1. Protecting other children 2. Furthering the data access rights of the child, 3. To ensure data that is within the scope of the IICSA is not prematurely deleted. https://www.iicsa.org.uk/ and https://www.iicsa.org.uk/key-documents/91/view/inquiry-opening-statement.pdf

Appendix 5

Useful Web Resources

Records Requests

- ICO Guidance – Data Protection Advice for Schools
  https://ico.org.uk/for-organisations/education/

- Subject Access Code of Practice
  https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf
  https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/

- Circular 18 /2006 Educational Records, School Reports and the Common Transfer System
  http://gov.wales/about/foi/publications-catalogue/circular/circulars2006/1552927/?lang=en

- Publication of Exam Results Guidance
  https://ico.org.uk/for-the-public/schools/exam-results/

- Pupil Information (Wales) Regulations 2011
  http://www.legislation.gov.uk/wsi/2011/1942/made

Data Breaches

- ICO Guidance – Data Security Breach Management
  https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf

- Art 29 Working Party Guidance on Personal Data Breach Notification
  http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

School – Data Protection Guidance Documents

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