Enw'r Ysgol / *Name of School*

Polisi Asesiad Effaith Diogelu Data Ysgolion (DPIA) / *Schools Data Protection Impact Assessment (DPIA) Policy*

(Fersiwn 1, Ebrill 2022 / *Version 1, April 2022)*

Ynglŷn â'r polisi hwn

Mae DPIA yn ddull strwythuredig o nodi'r risgiau preifatrwydd sy'n gysylltiedig â phrosesu data personol ac ar gyfer gweithredu rheolaethau priodol i reoli'r risgiau hynny.

Mae'r polisi hwn yn gosod y fframwaith ar gyfer asesiad ffurfiol i sicrhau bod prosesau a systemau newydd a gyflwynir yn bodloni rhwymedigaethau cyfreithiol o ran cyfrinachedd, diogelu data a diogelwch.

Cefnogir y polisi hwn gan adnoddau ar y dudalen Diogelu Data ar Feicrowefan y Gwasanaeth Dysgu.

About this policy

A DPIA is a structured approach to identifying the privacy risks associated with the processing of personal data and for implementing appropriate controls to manage those risks.

This policy lays the framework for a formal assessment to ensure that new processes and systems introduced meet legal obligations regarding confidentiality, data protection and security.

This policy is supported by resources on the Data Protection page on the Learning Service Microsite.

Fersiwn / *Version*	**Dyddiad / *Date***	**Crynodeb o newidiadau / *Summary of changes***	**Dyddiad a Dderbyniwyd gan Fwrdd o Lywodraethwyr / *Date Accepted by Board of Governors***
F1 / *V1*	Ebrill 2022 / *April 2022*	Polisi newydd / *New policy.*	30/09/26

Dyddiad yr adolygiad nesaf / *Date of next review*	
Bydd y polisi hwn yn cael ei adolygu yn: / *This policy will be reviewed in:*	Ebrill 2025 / *April 2025*
Yr unigolyn a fydd yn ymgymryd â'r adolygiad fydd: / *The review will be undertaken by:*	Swyddog Diogelu Data Ysgolion / *Schools Data Protection Officer*

Manylion Cyswllt:

Swyddog Diogelu Data Ysgolion

E-bost:
dpoysgolionmon@ynysmon.gov.uk

Rhif ffôn: 01248 751833

Cyfeiriad:
Gwasanaeth Dysgu
Cyngor Sir Ynys Môn
Swyddfeydd y Cyngor
Llangefni
Ynys Môn
LL77 7TW

Contact Details:

Schools Data Protection Officer

E-mail:
dpoysgolionmon@ynysmon.gov.uk

Telephone: 01248 751833

Address:
Learning Service
Isle of Anglesey County Council
Council Offices
Llangefni
Anglesey
LL77 7TW

Rydym yn hapus i ddarparu'r polisi hwn ar ffurfiau eraill ar gais. Defnyddiwch y manylion cyswllt uchod. / *We are happy to provide this policy in alternative formats on request. Please use the above contact details.*

Dogfen: Templed polisi ar y fframwaith ar gyfer asesiad ffurfiol i sicrhau bod prosesau a systemau newydd a gyflwynir yn bodloni rhwymedigaethau cyfreithiol o ran cyfrinachedd, diogelu data a diogelwch.

Document: *Policy template on the framework for a formal assessment to ensure that new processes and systems introduced meet legal obligations regarding confidentiality, data protection and security.*

Cyfrifoldeb: *Cyfrifoldeb llywodraethwyr yr ysgol a'r Pennaeth fel y Rheolydd Data yw sicrhau bod gweithdrefnau ar waith i sicrhau bod yr ysgol yn cydymffurfio â deddfwriaeth diogelu data. Cyfrifoldeb y Pennaeth yw sicrhau bod holl staff yr ysgol yn gweithredu ac yn cydymffurfio.*

Responsibility: *It is the responsibility of the school governors and Headteacher as the Data Controller to ensure procedures are in place to ensure that the school complies with data protection legislation. It is the responsibility of the Headteacher to ensure implementation and compliance by all school staff.*

Content **Page**

1. Policy Statement 23
2. Scope 23
3. Legislation, Guidance and Policies 23
4. Definitions 24
5. Responsibilities 25
   - 5.1. School Governing Body 25
   - 5.2. Headteacher (and/or Person Responsible for Data Protection within the School) 25
   - 5.3. All Staff within the School 25
   - 5.4. Schools Data Protection Officer 26
6. What is a Data Protection Impact Assessment (DPIA)? 26
7. Purpose of Data Protection Impact Assessments 27
8. Key Elements of a Data Protection Impact Assessment Process 28
9. Key Benefits of Data Protection Impact Assessments 28
10. Identifying the need for a Data Protection Impact Assessment 28
11. When Data Protection Impact Assessments must be Undertaken 29
12. Who should undertake a Data Protection Impact Assessment? 30
13. Consultation with Key Stakeholders 31
14. Assessing Impact 31
15. Outcomes of a Data Protection Impact Assessment 32
16. Steps to take following Completion of Data Protection Impact Assessment 33
17. Review of the Data Protection Impact Assessment 34
18. Consultation with the Information Commissioner's Office (ICO) where there is High Residual Risk 34
19. Legacy Systems or Technology 34
20. Staff Training 35
21. Breach of the Policy 35
22. Review of Policy and Oversight Arrangements 35

APPENDIX A- Schools Data Protection Risk Matrix 37
APPENDIX B- Schools Data Protection Impact Assessment (DPIA) Policy- Headteacher's Checklist 39

1. Policy Statement

The school is fully committed to protecting personal data in accordance with the requirements of the *UK General Data Protection Regulation (UK GDPR*) and the *Data Protection Act 2018.*

The *UK GDPR* includes an obligation to conduct a Data Protection Impact Assessment (DPIA) for types of processing likely to result in a *high risk* to individuals' interests.

This policy lays the framework for a formal assessment to ensure that new processes and systems introduced meet legal obligations regarding confidentiality, data protection and security.

The school will complete DPIAs, where appropriate, to demonstrate accountability and compliance with the *UK GDPR.*

2. Scope

This policy applies to all members of school staff, including temporary workers, contractors, volunteers, governors and partner organisations that introduce new processes or systems that are likely to involve a new use or significantly change the way in which personal data is handled and processed.

This policy also applies where a significant incident has occurred in relation to a current process/system or where existing processes are amended, such as undertaking current processing in different ways.

The school is committed to ensuring that a DPIA process is in place and that all new projects, processes and systems (including software and hardware) which are introduced, meet legal and statutory obligations regarding privacy, confidentiality, data protection and security.

This policy applies to all types of personal data held by the school.

The law requires that the Schools Data Protection Officer be consulted by the school as part of the DPIA process, and in order to assist to determine whether a DPIA is required or not.

3. Legislation, Guidance and Policies

The main data protection legislation that this policy complies with is that of the *UK General Data Protection Regulation (UK GDPR)* and the *Data Protection Act 2018.*

This policy is also based on relevant codes of practice and on guidance published by the Information Commissioner's Office (ICO).

This policy should also be read in conjunction with the *Schools Data Protection Policy; Schools Information Security Policy; Schools Data Processing Policy* and *Schools Retention Schedule.*

4. Definitions

Personal data	Any information relating to an identified or identifiable natural person that can be identified either directly or indirectly from that information. This can be stored electronically, on a computer, or in paper-based filing systems.
Special category data	Information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation. Special category data is personal data that needs more protection because it is sensitive.
Data controller	The people, or organisations, which determine the purposes for which, and the manner in which, any personal data is processed. The data controller has a responsibility to establish practices and policies in line with legislation. The school is the data controller.
Data processors	Includes any person who processes personal data on behalf of a data controller (other than the employee of the data controller). Data processors could include suppliers which handle personal data on behalf of the school.
Data subject	The individual to whom the personal information relates.
Processing information	Collecting, obtaining, recording, organising, structuring, storing, retaining, amending, adapting, altering, retrieving, consulting, disseminating, restricting, disclosing, destroying, erasing information or using or doing anything with it.
Risk	Effect of uncertainty on objectives. Risks to individuals: the potential for damage or distress. Risk is often characterised by reference to potential "events" and "consequences", or a combination of these.
Risk Assessment	The identification and analysis of risks to the organisation's business objectives.
Likelihood	How likely is it that the risk will occur- uncertainty, chance and probability.
Impact	What are the consequences of the risk were it to occur. Impact is considered as having either an immediate effect or a future effect.
Control	Measure that is modifying risk.
Genetic data	Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural

	characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. Fingerprint recognition is an example of dactyloscopic data.
Cloud storage	Cloud storage is a cloud computing model in which data is stored on remote servers accessed from the internet, or "cloud." It is maintained, operated and managed by a cloud storage service provider on storage servers that are built on virtualisation techniques.
Information Commissioner's Office (ICO)	The ICO is the UK's independent body (supervisory authority) set up to uphold information rights. The ICO's role is to uphold information rights in the public interest. This includes dealing with complaints regarding problems accessing personal information from an organisation, or if there are concerns about how an organisation has handled information- if the information is wrong, has been lost or disclosed to someone else. Data breaches that are a high risk to individuals are reported to the ICO.

5. Responsibilities

5.1. School Governing Body

The school governing body has the responsibility for:

- ensuring that this policy has been formally adopted by the school;
- monitoring the school's overall compliance and accountability relating to this policy;
- ensuring that the school can evidence compliance with data protection legislation.

5.2. Headteacher (and/or Person Responsible for Data Protection within the School)

The Headteacher and/or the person who is responsible for data protection within the school is responsible for:

- ensuring that school staff are aware of the DPIA process and fully comply with the policy;
- contacting the Schools Data Protection Officer when implementing or changing a process or system, in order to determine whether a DPIA is required or not;
- identifying key stakeholders that need to be consulted as part of the DPIA process;
- ensuring that the DPIA process is revisited should there be a substantial change to process or a significant privacy risk raised;
- integrating the outcomes of the DPIA into project plans;
- maintaining a log of all of the school's DPIAs as part of the *Record of Processing Activities (ROPA*);
- monitoring the ongoing performance of the DPIA;
- keeping a record of the risks within a Risk Register;
- publishing DPIAs if appropriate;
- ensuring that the DPIA is stored securely.

5.3 Staff within the School

Staff employed or volunteering within the school, including teachers, classroom assistants and business support staff are responsible for:

- complying with this policy to ensure that processing remains compliant with current legislation if implementing or changing a process or system;
- being able to identify when a DPIA may be required and to notify the Headteacher;
- undertaking any training provided regarding DPIAs if this is relevant to job role.

5.4. Schools Data Protection Officer

The Schools Data Protection Officer is responsible for:

- assisting the Headteacher to determine whether a DPIA is required or not when implementing or changing a process or system;
- assisting the Headteacher in completing a *DPIA Screening Checklist*;
- supporting the school to complete a DPIA;
- providing advice on what measures and safeguards the school can take to mitigate risks;
- confirming that the DPIA has been completed correctly;
- facilitating the process of consulting with the Information Commissioner's Office (ICO) where there is a high residual risk;
- providing advice on the outcome of the DPIA and whether the processing can go ahead;
- providing advice to the Headteacher regarding publishing DPIAs;
- providing advice and guidance in relation to reviewing DPIAs;
- providing advice and guidance relating to legacy initiatives or systems;
- maintaining a log of DPIAs on behalf of all schools;
- monitoring the DPIA's ongoing performance, including how well the school has implemented planned actions to address the risks;
- ensuring that all data processing agreements include the requirement for data processors to assist the school to document processing activities and to identify any associated risks;
- ensuring that the DPIA will link and comply with each of the Data Protection Principles;
- providing training on how to complete DPIAs to school staff who will be a part of completing DPIAs.

6. What is a Data Protection Impact Assessment (DPIA)?

A DPIA is a structured approach to identifying data protection risks associated with the processing of personal data; to help the school identify and minimise the risks and for implementing appropriate controls to manage them. **A DPIA is a legal requirement for processing that is likely to be *high risk*.**

The DPIA is an evaluation tool designed to systematically and comprehensively analyse, identify, minimise and address the data protection, privacy and security risks of

processing. A DPIA assesses the likelihood and impact of a compromise to the confidentiality, integrity and/or availability of personal data.

A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the *potential* for harm – to individuals or to society at large, whether it is physical, material or non-material.

The school will make an objective assessment of the risks and will use the *Schools Data Protection Risk Matrix* (APPENDIX A) to think about likelihood and severity of risks. The *Schools Data Protection Risk Matrix* is also available on the Data Protection page on the Learning Service Microsite.

All new projects, programmes, processes, information systems (including software and hardware) and other relevant information assets should be developed and implemented in a secure and structured manner and comply with legal and statutory requirements. They must comply with confidentiality, privacy and data protection requirements. All new processes or systems must be tested against these requirements before they are introduced.

To determine whether any proposed changes to the school processes and information assets impacts on the confidentiality, integrity and accessibility of personal and/or sensitive data, the school will utilise the DPIA to test against these requirements.

DPIAs will be imbedded into the school's processes and risk management framework. DPIA requirements are included in all relevant policies, processes and procedures.

The school will ensure the outcome can influence the school's plans. A DPIA is initiated and maintained throughout the development and implementation of a project, process or system.

7. Purpose of Data Protection Impact Assessments

The purpose of the DPIA is to highlight any privacy risks associated with a project or process and to ensure that the proposed uses of personal data are fully understood.

The DPIA reports and captures the details of potential impacts identified and the solutions or actions that will reduce the impact or mitigate the risk. The *UK GDPR* requires a level of assessment to be completed that is proportionate to the risks involved in the processing.

DPIAs are specifically mandated by the *UK GDPR* to assess the risks to data subjects' privacy and data protection rights arising out of the school's processing activities.

DPIAs are a legal requirement for processing that is likely to be *high risk*. An effective DPIA can also bring broader compliance; financial and reputational benefits; helping to demonstrate accountability and building trust and engagement with individuals.

8. Key Elements of a Data Protection Impact Assessment Process

A DPIA should begin early in the life of a project, process or system, ***before*** processing begins, and run alongside the planning and development process.

A DPIA should include these steps:

Step 1: identify the need for a DPIA;
Step 2: describe the processing;
Step 3: consider consultation;
Step 4: assess necessity and proportionality;
Step 5: identify and assess risks;
Step 6: identify measures to mitigate the risks;
Step 7: sign off and record outcomes.

The school will scale the time and resources needed for a DPIA to fit the nature of the process.

9. Key Benefits of Data Protection Impact Assessments

Key benefits of DPIAs include:

- fulfilling the school's statutory obligations;
- contributing towards effective risk management and increased privacy and data protection awareness across the school;
- giving individuals confidence that the school is taking steps to safeguard their privacy, and a better understanding of the ways in which their personal data is being used;
- improve the school's relationship with individuals and improve the school's understanding of individuals' needs, concerns and expectations;
- demonstrating that the school is taking actions which are less likely to be privacy intrusive and have a negative impact on individuals;
- ensuring that initiatives are likely to be successful because privacy risks are identified early, allowing controls to be designed at less cost and with less impact on delivery.

10. Identifying the need for a Data Protection Impact Assessment

To determine whether a DPIA is required, the school must identify whether personal data is being processed. Some examples of such information include:

- information linked or linkable to an individual;
- date of birth, place of birth, race, religion, weight, geographical indicators; employment, medical, education and financial information;

- name (e.g. full name, maiden name, mother's maiden name, or alias);
- address information (e.g. street or e-mail address);
- information identifying personally owned property (e.g. vehicle registration number);
- telephone numbers, mobile, and personal numbers;
- personal characteristics, including photo (face or distinguishing features), fingerprints, biometric data (retina scan, etc.);
- personal identification number (e.g. National Insurance Number, passport number, driver's licence, financial account or credit number).

11. When Data Protection Impact Assessments must be Undertaken

It is mandatory to undertake a DPIA before beginning any processing that involves personal data which is *likely to result in a high risk.* This ensures that privacy risks are identified and considered before they are implemented into the design and reviewed regularly throughout the lifecycle.

The *DPIA Screening Checklist* will be used as a preliminary stage to assist the school to determine when DPIAs are required.

Requirement for DPIAs is not restricted to formal projects. Risk to the privacy of individuals can arise in many scenarios or initiatives.

DPIAs may be required for proposals to undertake new processing of personal data or where existing processes are amended, such as undertaking current processing in different ways.

All new or significantly changed processes or projects that involve personal data that are planned to be introduced must comply with confidentiality, privacy and data protection legislation and requirements.

A DPIA will be undertaken in the early stages of an initiative. The law requires the school to undertake a DPIA if it intends to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data (sensitive data) on a large scale; or
- systematically monitor publicly accessible places on a large scale.

The ICO also requires the school to undertake a DPIA if it intends to:

- use new, innovative, technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data (e.g. facial recognition used to allow access to systems);
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing:

- them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

Examples of scenarios or initiatives which may require a DPIA include:

- a proposal to build a new IT system for storing or accessing personal data;
- implementing surveillance technology in a building, such as a CCTV system;
- using a cloud service for the storage of data;
- developing policies or strategies that have privacy implications.

The Headteacher will need to consider whether any processing requires a DPIA and will consult the Schools Data Protection Officer.

Factors to consider include whenever the processing:

- involves the collection of new information about individuals;
- uses information about individuals for a purpose it is not currently used for, or in a way it is not currently used;
- involves the use of new technology that might be perceived as being privacy intrusive;
- may result in making decisions, or taking action against individuals in ways that can have a significant impact on them;
- involves information about individuals of a kind particularly likely to raise privacy concerns or expectations such as vulnerable individuals.

Children are regarded as vulnerable to the processing of their personal data since they may be less able to understand how their data is being used, anticipate how this might affect them, and protect themselves against any unwanted consequences.

If there is uncertainty regarding whether it is appropriate to carry out a DPIA for a specific project, process or system, the Headteacher should consult the Schools Data Protection Officer for clarification and advice.

12. Who should undertake a Data Protection Impact Assessment?

The school as the data controller is ultimately responsible and accountable for compliance with data protection legislation. The Headteacher is responsible for ensuring that DPIAs are undertaken. It is important that staff are able to identify when a DPIA may be required and to notify the Headteacher.

The Headteacher will consult the Schools Data Protection Officer as part of the DPIA process, and in order to assist to determine whether a DPIA is required or not. The Schools Data Protection Officer must provide advice and input.

A DPIA should be conducted by the process owner and assisted by those involved in the business process that have the right knowledge and a strong understanding of the process itself along with the Headteacher and the Schools Data Protection Officer. It may also be appropriate to seek legal advice or advice from other independent experts such as IT experts, where appropriate.

If the school uses any data processors, the school will ask them to provide information, assistance and input where appropriate (and if applicable). Data processors will document their processing activities and identify any associated risks. Any contracts with data processors will note the requirement to assist. The school will remain responsible for the DPIA as the data controller.

13. Consultation with Key Stakeholders

Consultation may be required as part of the DPIA. Consultation with key stakeholders can serve many purposes throughout the DPIA process, such as:

- explaining the initiative to stakeholders;
- explaining to stakeholders how the DPIA process will be used within the initiative to manage privacy risks;
- establishing current working practices that the initiative aims to update or replace;
- establishing how the new system or process is likely to be used in practice and in the case of general purpose facilities, their likely purpose;
- establishing the privacy concerns of stakeholders;
- soliciting suggestions for controls;
- explaining identified controls to stakeholders.

Key stakeholders are likely to include:

- individuals who understand the initiative from a technical point of view and in terms of personal data processing;
- individuals who will be using the new system or process;
- individuals whose personal data will be processed by the new system or process;
- collaborative partners;
- the suppliers of a system.

Where appropriate, the school will seek and document the views of individuals or their representatives on the intended processing, unless there is a good reason not to. If it is decided that this is not appropriate, a record of this decision, with a clear explanation, will be documented as part of the DPIA.

The school will also document if the DPIA decision differs from the views of individuals, and will document the reasons for disregarding their views or the views of other consultees.

14. Assessing Impact

The DPIA will consider the potential impact on individuals and any harm or damage that might be caused by processing, including:

- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification or de-identification of data; or
- any other significant economic or social disadvantage.

15. Outcomes of a Data Protection Impact Assessment

The DPIA will provide details around the outcomes of the assessment, including:

- a description of the nature, scope, context and purposes of the processing;
- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the school;
- an assessment of the necessity and proportionality and compliance measures of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of individuals; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance, taking into account the rights and legitimate interests of data subjects and other persons concerned.

The DPIA will:

- identify the data protection implications of the process/system;
- consider the impacts or processing from the perspectives of all stakeholders;
- identify ways in which negative impacts on privacy can be avoided;
- identify ways to lessen negative impacts on privacy;
- provide clarity as to the business need for processing where negative impact on privacy is unavoidable.

The DPIA will record:

- what additional measures are planned;
- whether each risk has been eliminated, reduced or accepted;
- the overall level of ‘residual risk’ after taking additional measures;
- whether the ICO needs to be consulted;

- responses to the views of data subjects and any other consultees, including the Schools Data Protection Officer.

The DPIA will link to the Data Protection Principles and the Data Protection Principles will be applied throughout the lifecycles of the process:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specified, explicit and legitimate purposes;
3. Adequate, relevant and limited to what is necessary (data minimisation);
4. Accurate and, where necessary, kept up to date;
5. Retained only for as long as necessary;
6. Processed in an appropriate manner to maintain security.

The DPIA will explicitly state how the school is complying with each of the Data Protection Principles under *UK GDPR* and clearly explain the lawful basis for processing.

16. Steps to take following Completion of Data Protection Impact Assessment

It is the responsibility of the Headteacher to ensure that the DPIA is stored securely.

The school will integrate the outcomes of the DPIA into project plans. Action points will be identified and who is responsible for implementing them.

The school will monitor the ongoing performance of the DPIA.

A DPIA does not have to indicate that all risks have been eradicated. But it should help the school document them and assess whether or not any remaining risks are justified.

If the school decides to accept a high risk, either because it is not possible to mitigate or because the costs of mitigation are too high, the school will consult the ICO before going ahead with the processing. The school does not always have to eliminate every risk. It may be decided that some residual risks, and even a high risk, are acceptable given the benefits of the processing and/or the difficulties of mitigation.

The school will keep a record of the risks within a Risk Register. The Risk Register will record, assess and monitor the identified risks. A Risk Register template is available on the Data Protection page on the Learning Service Microsite.

It is good practice for the school to publish DPIAs. If the school is concerned that publication may reveal commercially sensitive information, undermine security or cause others risks, the school will consider removing sensitive details if necessary, or publish a summary.

As part of the sign-off process, the Schools Data Protection Officer will advise on whether the processing is compliant and can go ahead. The Schools Data Protection Officer's advice will be recorded in the DPIA. If the school doesn't follow the Schools Data Protection Officer's advice, reasons should be recorded and the school needs to ensure it can justify its decision.

17. Review of the Data Protection Impact Assessment

The school will have a process in place to keep DPIAs under ongoing review to ensure they remain relevant. Data protection and privacy risks should be monitored throughout the process management cycle and the measures that have been put in place will be reviewed. A DPIA should be seen as an ongoing process with regular reviews based on the level of risk and the nature of the processing activity.

The Headteacher should ensure that the DPIA process is revisited should there be a substantial change to process or a significant privacy risk raised.

The DPIA will need to be repeated if there is a substantial change to any of the following in relation to processing being undertaken- nature; scope; context; purpose of the processing and lawful basis for processing.

DPIAs need to assess any new risks if there are any significant changes in why the school processes personal data or in the amount of data collected. An external change to the wider context of the processing should also prompt the school to review the DPIA.

The Schools Data Protection Officer will provide advice and guidance in relation to reviewing DPIAs.

18. Consultation with the Information Commissioner's Office (ICO) where there is High Residual Risk

In the event that the results of the DPIA indicate the processing would result in a high level of residual risk to individuals that cannot be mitigated, the law requires that the ICO is consulted *before* any processing takes place.

The ICO does not expect that every DPIA will be sent to them, but the ICO must be consulted if the DPIA identifies high risks and the school cannot take measures to reduce those risks. The Headteacher should consult the Schools Data Protection Officer for advice and to facilitate this process.

When a consultation is started, the ICO will provide written advice within 8 weeks, although in complex cases, the period may be extended to a maximum of 14 weeks. If the response time is extended, the ICO will issue a notification within one month of the date the DPIA was submitted and explain its reasons.

The ICO will provide a judgement on the proposed processing and, if appropriate, give details of what must be done to make the processing acceptable under the *UK GDPR*; issue a formal warning not to process the data, or ban the processing altogether.

The school cannot begin the processing until the consultation has been completed.

19. Legacy Systems or Technology

The school does not require all legacy initiatives or systems to have a DPIA, however they are a useful tool to provide assurance of data protection compliance and can be implemented if it is appropriate.

For processes that have already undergone a PIA under the *Data Protection Act 1998*, it is only necessary to conduct a DPIA if there has been a significant change to the nature, scope, lawful basis, context or purposes of the processing since the previous assessment under previous legislation.

It is recommended that a DPIA is conducted where a processing operation has not had a previous assessment and where the processing is likely to result in a high risk to the rights and freedoms of natural persons.

The school will document reasons for not conducting a new DPIA where relevant so that the school can demonstrate compliance with legislation.

The Schools Data Protection Officer will provide advice and guidance relating to legacy initiatives or systems.

20. Staff Training

The Schools Data Protection Officer will provide training on how to complete DPIAs to school staff who will be a part of completing DPIAs.

21. Breach of the Policy

Non-compliance with this policy by members of school staff could lead to serious consequences.

This can lead to putting both the individuals whose personal information is being processed and the school at risk.

If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

22. Review of Policy and Oversight Arrangements

This policy will be reviewed by the Schools Data Protection Officer every three years, unless changes to legislation, codes of practice, policy or guidance requires the policy to be updated sooner.

This policy will be approved by the Learning Service Senior Management Team and will be adopted by the school governing body. Compliance with this policy and related procedures will be monitored by the School Leadership Team and the governing body.

If there are any queries or concerns about anything contained in this policy, the Schools Data Protection Officer should be contacted without hesitation:

E-mail: dpoysgolionmon@ynysmon.gov.uk

Telephone: 01248 751833

Address:
Learning Service
Isle of Anglesey County Council
Council Offices
Llangefni
Anglesey
LL77 7TW

Further information regarding Data Protection Impact Assessments can be obtained from the ICO website: https://ico.org.uk

APPENDIX A- Schools Data Protection Risk Matrix

LIKELIHOOD									
	Event is almost certain to occur in most circumstances	**>70%**	**Almost certain**	**A**					
	Event likely to occur in most circumstances	**30-70%**	**Likely**	**B**					
	Event will possibly occur at some time	**10-30%**	**Possible**	**C**					
	Event unlikely and may occur at some time	**1-10%**	**Unlikely**	**D**					
	Event rare and may occur only in exceptional circumstances	**<1%**	**Rare**	**E**					
					5	**4**	**3**	**2**	**1**
					Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
			Data Protection Consequences		Affects a minimal number of data subjects.	May involve a small number of data subjects – no sensitive data.	May involve some data subjects or relates to sensitive data.	May affect a large amount of data subjects. Remediation is likely to be time consuming and complex.	Affects a significant numbers of data subjects. Remediation is likely to be time consuming and complex, tracked at a senior level and related to sensitive information.
					IMPACT				

Risk Severity Key

	Minor	Risk easily managed by the Headteacher
	Moderate	Risk containable by the Headteacher – School Governing Body may need to be informed
	Major	Intervention by the School Governing Body and / or Learning Service Senior Management involvement
	Critical	Significant School Governing Body and Learning Service Senior Management intervention

APPENDIX B

Schools Data Protection Impact Assessment (DPIA) Policy

Headteacher's Checklist

No	Actions to be Taken	Has the school got this in place (Yes/No)/ Comments/Dates etc.)
1	The current version of the *Schools Data Protection Impact Assessment (DPIA)* has been formally adopted by the School Governing Body.	
2	There is a process in place to continually monitor the school's compliance with this policy.	
3	The Schools Data Protection Officer has been contacted when considering implementing or changing a process or system, in order to determine whether a DPIA is required or not- this is for any app, system, programme or service where personal data is being processed. To contact the SDPO **before** purchasing and at the **very beginning of the process**.	
4	All of the school's DPIAs are recorded on the school's *Record of Processing Activities (ROPA*) and this is kept up-to-date and includes any changes/amendments relating to DPIAs.	
5	A record of all of the risks identified within DPIAs are recorded in a Risk Register. The risks are monitored and the Risk Register is kept up-to-date.	
6	All DPIAs are stored securely on the school's IT system and they can be easily accessed when needed.	
7	Key stakeholders that need to be consulted as part of the DPIA process are identified.	
8	DPIAs are published where this is considered appropriate.	
9	The ongoing performance of the DPIA is monitored.	