YSGOL Y FAENOL

Polisi Diogelu Data 2022
Rheoliad Diogelu Data Cyffredinol (GDPR) a Deddf Diogelu Data 2018

Data Protection Policy 2022
General Data Protection Regulation (GDPR) and the Data Protection Act 2018

Dyddiad Cymeradwyo/Date Adopted: 02.10.25
Dyddiad Adolygu/Review Date: 01.10.26

Llofnodwyd ar ran Cadeirydd y Llywodraethwyr: _____

Dyddiad: _____

Table of contents

1. Document history

1.1 Revision history

Date	Version	Author	Revision Summary

1.2 Review by Data Protection Officer (DPO)

This DPIA has been reviewed by the DPO on these dates:

Date	Version Number of DPIA	DPO Comments

1.3 Approval

This document requires approval from **Information Asset Owner** named below:

Date	Version	Name

2. Screening Questions

To be completed by the task lead

Please complete the table below. **Answering "Yes" to any of the screening questions below represents a potential IG risk factor** that will have to be further analysed to ensure those risks are *identified*, *assessed* and *mitigated* wherever possible by working through **sections A**, **B** and **C** of this document.

Category	Screening question	Yes/No
Identity	Will the task involve the collection of new information identifiable about individuals?	
Identity	Will the task compel individuals to provide personal information about themselves?	
Multiple organisations	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
Data	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
Data	Does the task involve using new technology which might be perceived as being privacy intruding for example biometrics or facial recognition?	
Data	Will the task result in you making decisions or taking action around individuals in ways which could have a significant impact on them?	
Data	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example health records, criminal records, or other information that people are likely to consider as private? Also vulnerable individuals eg children	
Data	Will the task require you to contact individuals in ways which they may find intrusive?	
Storage	Will the information/task be stored in the cloud? (I*f answer is yes please complete the questions on cloud (page 9 onwards)*	
Systems	Have you discussed technical requirements (*if applicable*) with IT?	
Systems	Has an *IT Technical Specification* been completed by the supplier / provider?	

3. Privacy Impact Assessment

Section A - Task Description

To be completed by the task lead

Please complete with as much information as possible as this will assist the DPO in assessing whether further action is required.

Task Name:	
Directorate/Department:	
Is this a change to an existing process?	
Assessment Completed by:	
Job Title:	
Date completed:	
Phone:	
E-mail:	
Information Asset Owner:	
Task/Change Outline - *What* is it that is being planned?	
Purpose / Objectives - *Why* is it being undertaken? This could be the objective of the process or the purpose of the system being implemented as part of the task.	
What is the purpose of collecting the information within the system? For example research, audit, reporting, staff administration etc.	
Provide a description of the information flows. Even if detailed information is not available some indication must be provided; this may already be available through requirements gathering. Broadly speaking the aim is to establish: **who** the information will be made available to, **what** type of information, **why** the information is required, **how** it will be shared and **how often**.	

Provide details of how the proposal will have the potential to impact on the confidence service users have in the Council maintaining the confidentiality of their personal data. For example, it could be that specific information is being gathered or used that hasn't been used or gathered previously; the level of information held about an individual is increasing or information is being shared with another organisation through a shared system or database where it wasn't previously.
Provide details of any previous Data Protection Privacy Impact Assessment or other form of personal data compliance assessment done on this initiative. If this is a change to an existing system, a DPIA may have been undertaken during the task implementation.
Stakeholders - who is involved in this task/change? Please list stakeholders, including internal, external, organisations (public/private/third) and groups that may be affected by this system/change in the table below and detail any stakeholder activity taken.

Organisation	Engagement / Stakeholder Activity

Stakeholders - Has there been any consultation with data subjects (the individuals that the system or proposed change will affect or impact)?
☐**Yes** **How was this done?** …… ☐**No**

Data Types

In order to understand the potential risks to individual's privacy, it is important to know the types of data that will be held and/or shared. Even if exact detail is not known and initial indication will assist in the privacy impact assessment.

Personal	Tick (All that Apply)	Special Category	Tick (All that Apply)
Name	☐	**Racial / ethnic origin**	☐
Address (home or business)	☐	**Political opinions**	☐
Postcode	☐	**Religious beliefs**	☐
NHS No.	☐	**Trade union membership**	☐
Email address	☐	**Physical or mental health**	☐
Date of birth	☐	**Sexual life**	☐
Reference number If ticked, please detail:	☐	**Genetic data / Biometrics; DNA profile, fingerprints**	☐
Driving Licence [shows date of birth and first part of surname]	☒		
Bank, financial or credit card details	☐		
Mother's maiden name	☐		
National Insurance number	☐		
Tax, benefit or pension Records	☐		
Criminal offences	☐		
Employment, school, Social Services, housing records	☐		
Data of a "higher" sensitivity (tick all that apply)			
Health condition information	☐	**Genetic**	☐
Mental Health	☐	**Adoption**	☐
Child Protection	☐	**Safeguarding Adults**	☐
Comments and Additional data types (if relevant):			

Section B – Privacy Impact Assessment Table [insert task name]

The **task lead** should complete the '*Response'* box for each question. The DPO will then complete the 'Risk Type' and 'Outcome' box

Guidance Notes:

Response - Please answer the questions as fully as possible. If you are unsure of how to answer the question, **please contact the Data Protection Officer (DPO).** If there is supporting information that relates to any of the questions, which you feel would be informative, indicate within the comments section and send this along with the completed assessment.

Additional guidance notes have been provided for some questions; once completed the guidance notes can be removed.

The assessment table is designed to be a 'working document' that can be added to at intervals throughout the process, for example bullet points or rough notes can be used. These notes can be used to highlight things that need to be followed up; noted requirements can be marked up ready for the requirement schedule, etc.

Risk Type – The DPO will use the guidance notes in Appendix 1 to identify the type of risk, this will help the organisation to judge the level of risk and either accept it or put in place appropriate measures to mitigate it.

Outcome – The DPO will use the information provided to decide if any potential IG risks are identified. If, following discussion with the task manager/lead it is agreed there is an IG risk that requires further action / management, the required actions will be noted on the DPIA. The risk will be scored and progress against the identified mitigations captured using a red/amber/green status. **If the DPIA identifies high risks and you are unable to take measures to reduce the risk, it is necessary to consult the Information Commissioner's Office before processing commences.**

1	Is there any data stored in the cloud?		
	Guidance Note: *Please complete*		
	Response (completed by task lead)	**Risk type (completed by DPO)**	**Outcome (completed by DPO)**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
2	Where will the information be held and who will have responsibility for it?		
	Guidance Note: *Detail which team or organisation has responsibility for the system that holds the data. Detail which team or organisation has responsibility for the storage of the data. Detail how the servers are configured and Resilient. Detail which team or organisation is responsible for the security of the server the data is located on. Where is the server located physically?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
3	What types of information will be held and/or shared?		
	Guidance Note*: For example a care plan, case correspondence, occupational health data.* *Will the records be electronic or paper?*		
	Response	**Risk type**	**Outcome**

	Type here	☐ Individual ☐ Organisational ☐ Compliance	

4	Will any of the following activities be involved (tick those that apply): ☐ Recording of demographic data ☐ Sharing of personal data ☐ Transfer of service user identifiable data: to other systems, to other third parties ☐ Other

5	What legal basis for processing will you be relying on? Please tick one for personal data and one for special category data (if processing). Please speak to your information governance team if unsure.			
	Personal Data		**Special Category Data (includes health data)**	
	Task carried out in the public interest or in the exercise of official authority – Art 6(1)(e)	☐	Provision of preventative or occupational medicine, health or social care or treatment, or the management of health or social care systems – Art 9(2)(h)	☐
	Protection of vital interests – Art 6(1)(d)	☐	Vital interests of the data subject or a third party where they are incapable of giving consent – Art 9(2)(c)	☐
	Necessary for compliance with a legal obligation – Art 6(1)(c)	☐	Necessary for reasons of substantial public interest - Art 9(2)(g)	☐
			Public health - Art 9(2)(i)	☐
	Consent – Art 6(1)(a)	☐	Explicit Consent – Art 9(2)(a)	☐
	Other (please detail)	☐	Research – Art 9(2)(j)	☐
			Other (please detail)	☐
	Outcome			

6	Will the planned use of personal data be covered by information already provided to individuals or is a new or revised communication planned or required?		
	Guidance Note: *'Fair Processing' i.e. informing individuals of what is happening to their information is a requirement under Data Protection Legislation. What are the existing communications? What are the planned communications?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
7	Will the development enable the sharing of records with other organisations? How will records be shared?		
	Guidance Note*: Will information be transferred to a central hub with a collated record made available to participating organisations? Will participating organisations be provided with a view of records created in another organisation?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
8	Will the development result in the handling of a significant amount of new data about each person, or significant change in existing data holdings? Please detail the new data handled.		
	Guidance Note*: i.e. Is more information held about the same population of service users?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
9	Will the development result in the handling of **new data** about a significant number of people, or a **significant change in the population coverage**?		
	Guidance Note*: Please complete.*		

	Response	Risk type	Outcome
	Type here	☐ Individual ☐ Organisational ☐ Compliance	

10	Does the task involve **new linkage** of personal data with other data sets, or significant change in data linkages? Please list the linking systems		
	***Guidance Note**: Is the development dependent on, or does it link to other systems such as Welsh Demographic Service, NHS system? Will the NHS Number be used as the common identifier? How will records be matched / linked. What measures will be in place to correctly match/link records?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	

11	What security controls will be in place to prevent unauthorised or unlawful processing of information?		
	***Guidance Note:** Describe any such measures (e.g. system controls such as role based access, audit notifications, etc.) and outline any possible implications?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	

12	How is access to the system managed?		
	***Guidance Note**: Who authorises accounts, manages role based access and disables accounts? Please detail who is responsible for the business processes*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	

13	What additional controls will be in place to deal with information of a higher sensitivity?		
	Guidance Note: *Consideration must also be given to name changes through adoption, public protection or gender change and records relating to genetics, mental health, and occupational health.*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
14	What are the retention periods for the personal information and how will this be implemented?		
	Guidance Note*: Within the record keeping system, there must be a method of deciding 'what is a record?' and therefore 'what needs to be kept?' This is described as 'declaring a record'. A declared record is then managed in a way that will hold it in an accessible format until it is appraised for further value or it is destroyed, according to retention policy that has been adopted.*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
15	How will you action requests from individuals for access to their personal information (in accordance with their rights)?		
	Guidance Note*: Under relevant Data Protection legislation, individuals have a right to ask for a copy of information held about them. If this is a shared record it must be established who will be responsible for dealing with the request.*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
16	Will there be any secondary use of personal information in an identifiable or non-identifiable form?		

	Guidance Note: *Will the information be used for anything other than the main stated purpose? What level of information is to be used for these purposes, how will it be managed and how it will be communicated to service users?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
17	How are users to be trained in their information governance responsibilities? Have any training needs been identified in addition to the mandatory Council data protection training? Please detail training in full.		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
18	Is the information you are using likely to be of good enough quality for the purpose it is used for?		
	Guidance Note*: Consider the flow process, and how often, the information is checked for accuracy and are there procedures to support this? Is there is a facility to deal with data inaccuracies? Is there a facility to record the source of the information?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
19	Will the task involve any data migration or transfer of records from other systems/new feeds? If so, will the system origin and whether they were digitally born be captured in the metadata as part of the transfer process?		
	Guidance Note: *If the task involves any data migration, new feeds? If so, what are the identifiers used? Will the data be maintained in an accessible format? Will the relevant metadata be captured such as whether the information is scanned in, the author, scanner, transcriber, system origin etc.*		
	Response	**Risk type**	**Outcome**

	Type here		
20	Does the system maintain a comprehensive audit trail of user activity and how will the audit log be accessed and analysed?		
	Guidance Note: *Who will be responsible for auditing? Will additional or new organisational processes be required to meet the requirement to audit all user access?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
21	Will the information be transferred (electronically, physically or by other portable means) to an organisation outside of the Council? Please list the organisations.		
	Guidance Note: *Where will it go and what security arrangements will apply (e.g. encryption)? Will removable media be used? How will the information be transported (e.g. telephone, post, secure file sharing portal, email)?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
22	Are there business continuity and disaster recovery plans in place to recover information which may be damaged or lost through human error, computer virus, network failure, theft, fire, flood or other disaster?		
	Guidance Note: *Has this been agreed as part of the Service Management arrangements?*		
	Response	**Risk type**	**Outcome**

	Type here	☐ Individual ☐ Organisational ☐ Compliance	
23	Are there any elements of the system or service that are provided by a third party?		
	Guidance Note: *Is there a contractor (and any sub-contractors?) If so please document who the contracting authority is, who the contractors are and the confidentiality provisions within the contract, please note whether the procurement has been subject to information governance input, and whether the organisation is registered with the information commissioner*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
24	Does the development involve the use of new or inherently privacy invasive technologies?		
	Guidance Note: *For example: smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies and intelligent transportation systems, visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic.*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
25	Is automated decision making involved?		
	Guidance Note: *Is there any profiling involved? Can there be any human intervention if required?*		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	

26	One of the principles of data protection is to process no more personal data than necessary. Is all information being processed by the task necessary?		
	Response	**Risk type**	**Outcome**
	☐Yes ☐No If no, please detail Type here ……	☐ Individual ☐ Organisational ☐ Compliance	
27	Has this task been detailed on the information asset register?		
	Response	**Risk type**	**Outcome**
	Type here	☐ Individual ☐ Organisational ☐ Compliance	
Name ……			Date: ……

Section C – IG Requirements Schedule [insert task name]

The requirements schedule forms part of the Data Protection Impact Assessment (DPIA) process. This document must be read in conjunction with the task description for [insert task name] (section A)

Following the review of the populated DPIA table (section B) the DPO and task lead/manager will agree the information governance / privacy requirements and record them on the IG requirements schedule. Each requirement will be scored against the risk matrix at Appendix 3. The requirements schedule will be used to capture progress against each requirement and note the final outcomes. It should be stated whether the risks identified have been eliminated, reduced or accepted.

The schedule is designed to be a living document which is updated regularly as the development progresses.

Using red, amber and green (RAG) as progress indicators within the schedule, by the time the task goes live all requirements should be green. However, dependent on the nature of the task and the issues raised it is possible that requirements may be amber or in an exceptional case even red; where this is the case the organisations involved must agree to accept any residual risk.

See Appendix 2 for further guidance on how to complete the requirements schedule.

Ref	Question No.	Identified Requirement	Risk Assessment					Time-scale	Lead	Completion (RAG)	Comments / Progress / Further Action / Final Outcome
			Risk History	Likelihood	Impact	Score	Status (low, moderate, high,				
RQ1			Initial								
			Residual								
RQ2			Initial								
			Residual								
RQ3			Initial								
			Residual								
RQ4			Initial								
			Residual								

Are any residual risks scored higher than 10?

☐Yes ☐No

If Yes, has the ICO been consulted on the processing? ☐Yes ☐No
If the ICO has not been consulted on the processing and a residual risk is scored higher than 10, please state the reasons for not consulting the ICO below.

4. Appendices

Appendix 1 – Risk Type

Risk Type – this is the 'classification' as noted on the DPIA table (risk to individuals, compliance risk, organisation/corporate risk) and is noted in Section B.

Risks to individuals	Compliance risk	Associated organisation/corporate risk
• Inadequate disclosure controls increase the likelihood of information being shared inappropriately. • The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge. • New surveillance methods may be an unjustified intrusion on their privacy. • Measures taken against individuals as a result of collecting information about them might be seen as intrusive. • The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect. • Identifiers might be collected and linked which prevent people from using a service anonymously. • Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information. • Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised. • Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.	• Non-compliance with the common law duty of confidentiality • Non-compliance with the duties in the Health & Social Care (Safety & Quality) Act 2015 • Non-compliance with the relevant data protection legislation • Non-compliance with the Privacy and Electronic Communications Regulations (PECR). • Non-compliance with sector specific legislation or standards. • Non-compliance with human rights legislation.	• Non-compliance with the relevant data protection legislation or other legislation can lead to sanctions, fines and reputational damage. • Problems which are only identified after the task has launched are more likely to require expensive fixes. • The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation. • Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business. • Public distrust about how information is used can damage an organisation's reputation and lead to loss of business. • Data losses which damage individuals could lead to claims for compensation.

Risks to individuals	Compliance risk	Associated organisation/corporate risk
• If a retention period is not established information might be used for longer than necessary.		

Appendix 2 - Additional Guidance notes for completion of the Requirement Schedule

- **Ref -** Unique number allocated to each requirement (RQ) within the schedule, the reference number should be noted against the relevant question in the DPIA table.
- **Identified Requirement –** Details of the IG requirement identified and a brief description of the risk posed if the requirement is not addressed.
- **Risk History** – This is the status of the risk, whether it is the initial risk or the residual risk
- **Likelihood** – What is the likelihood of breaching relevant data protection legislation if no action is taken? This should be scored as per the table below.
- **Impact** – This is the severity of the impact of a breach of relevant data protection legislation if no action is taken. This should be scored as per the table below.
- **Score** – This is the *likelihood score* x *the impact score*.
- **Status** – This is whether the risk is **low**, **medium**, **high** or **extreme**. The score dictates the status as per the table below.
- **Timescale** – For each requirement to be addressed within, as aligned to the task timescales;
- **Lead** – Person responsible for taking each requirement forward;
- **Completion (RAG)** – The level of progress applicable to that action in red (for not begun), amber (in progress), green (complete)
- **Comments / Progress / Further Action / Final Outcome** describe the progress to date for each requirement (each entry should be dated), list any additional comments and further actions as appropriate. Ensure that it is noted if a risk has been eliminated, reduced or accepted. Any significant actions should be fed in as a further requirement.

Appendix 3 - Risk Scoring Tables

Likelihood score	1	2	3	4	5
Descriptor	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost certain**
Frequency How often might an IG breach occur	This will probably never happen/recur	Do not expect it to happen/recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur but it may not be a persisting issue	Will undoubtedly happen/recur,possibly frequently

Impact score (severity levels) and examples of descriptors	1	2	3	4	5
	Negligible	**Minor**	**Moderate**	**Major**	**Catastrophic**
Impact on an individual's privacy and confidentiality	Minimal privacy impact requiring no/minimal intervention Other manual or electronic process in place to mitigate the IG risk	Minor impact on an individual's privacy Other manual or electronic process in place to mitigate the IG risk	Moderate privacy impact requiring professional intervention Aspects of reputational damage for the organization if IG requirement not adopted Could result in an event which impacts on a moderate (less than 100) number of individuals	Major breach leading to possible larger scale privacy breaches Mismanagement of patient/client privacy with long-term reputational issues Would impact on over 100 individuals – part system failure	Serious IG breach and non-compliance with the law if requirement not adhered to An event which impacts on a large number of individuals – full system breach because of no adherence to standards. Is likely to be 1000 of individuals

		Likelihood				
		1	**2**	**3**	**4**	**5**
		Rare	**Unlikely**	**Possible**	**Likely**	**Almost certain**
Impact Score	**5 Catastrophic**	5	10	15	20	25
	4 Major	4	8	12	16	20
	3 Moderate	3	6	9	12	15
	2 Minor	2	4	6	8	10
	1 Negligible	1	2	3	4	5

Status

1 - 3	Low risk
4 - 6	Moderate risk
8 - 12	High risk
15 - 25	Extreme risk