Data Protection Impact Assessment Policy

Version 1
2022

Policy Document Control:

Organisation	Crickhowell High School
Title	Data Protection Impact Assessment Policy
Author	Professional Lead - Data Protection
Owner	Crickhowell High School
Subject	Schools Information Governance (IG) Policy
Protective Marking	No protective marking
Version	1
Review Date	August 2024

Revision History:

Revision Date	Revision	Previous Version	Description of Revision
10/03/2022	Non	N/A	Draft 1.

Policy Contents:

1. Definitions:

1.1. *UK General Data Protection Regulations ('UK GDPR')/Data Protection Act 2018 ('DPA 2018')* – In effect, these are regulations that lay down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

1.2. *Personal Data* – Any information relating to an identified or identifiable natural person ('data subject'); [directly or indirectly identified], 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.

1.3. *Special Category data* – Personal data that is of a more sensitive nature, such as information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

1.4. *Controller* – The body which, alone or jointly with other bodies, determines the purposes and means of the processing of personal data.

1.5. *Processor* – The body which processes personal data on behalf of the controller.

1.6. *Processing* – Covers a wide range of operations performed on personal data, including by manual or automated means. It includes the collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, erasure or destruction of personal data.

1.7. Data Protection Officer (DPO) – An individual appointed by the controller to assist a controller monitor internal compliance, inform and advise of a controller's data protection obligations, provide independent advice regarding Data Protection Impact Assessments and act as a contact point for data subjects and the Information Commissioner's Office.

2. Policy Introduction and Statement:

2.1. A Data Protection Impact Assessment (DPIA) is a method to help identify, analyse and minimise the data protection risks of a new or existing project or a change in a process when it is expected that the processing of personal data will result in a high-risk.

2.2. As a controller, the School will undertake a DPIA in an effort to consider data protection 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 will be on the potential harm to individuals or to society at large, whether it is physical, material or non-material.

2.3. DPIAs are a legal requirement, but the School recognises that an effective assessment can help demonstrate accountability and build trust and engagement with individuals.

2.4. For this policy to be its most effective, the School will follow it at the very early planning stages of new projects and ensure that it runs alongside the project plan.

3. Policy Purpose:

3.1. This policy will define when a DPIA is required and what information should be included within an assessment.

3.2. This policy will highlight what 'high-risk' is.

3.3. This policy will ensure that the School understands their legal obligation to undertake a DPIA when they propose to introduce a new project or process that is likely to result in a high risk to personal data.

3.4. The consequences of failing to abide by this policy, and choosing not to complete, or just generally having a disregard towards DPIAs will mean that the risks of processing personal data will not be identified nor understood, resulting in an inability to put in place mitigation plans to reduce those risks, potentially leading to the mishandling of personal data. In turn, this can lead to personal data breaches, increased data protection complaints, loss of public confidence, reputational damage including embarrassment and, in some cases, regulatory action from the Information Commissioners Office (ICO) including fines, in addition to requiring costly changes to a process or system.

4. Scope:

4.1. This policy applies to all School staff, contractual third parties or other individuals who process personal data to which the School is controller of.

4.2. The School will expect its processors/providers to feed into a DPIA when requested, for example, to provide or advise on technical details of a new system.

4.3. All users must understand and adopt the use of this policy when they propose to introduce a new project that is likely to result in a high-risk to personal data.

5. Responsibilities:

5.1. The Head Teacher and Chair of Governors have overall responsibility for ensuring the Schools compliance with this policy.

5.2. Each Head of Department is responsible for ensuring that DPIAs are undertaken as appropriate on data processing activities within their area (in consultation with the DPO).

5.3. The DPO shall provide advice and assistance on all DPIAs but is not responsible for the Schools compliance with this policy.

6. When is a DPIA required?

6.1. Before carrying out a full assessment, the School will answer a set of screening questions to identify whether or not the project will actually process personal data that will result in a high-risk.

6.2. The screening question will ask whether the project will:

6.2.1. use systematic and extensive profiling with significant effects;
6.2.2. process special category or criminal offence data on a large scale; or
6.2.3. systematically monitor publicly accessible places on a large scale.
6.2.4. use innovative technology;
6.2.5. use profiling or special category data to decide on access to services;
6.2.6. profile individuals on a large scale;
6.2.7. process biometric data;
6.2.8. process genetic data;
6.2.9. match data or combine datasets from different sources;
6.2.10. collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines);
6.2.11. track individuals' location or behaviour (in combination with any of the criteria from the European guidelines);
6.2.12. profile children or target marketing or online services at them; or
6.2.13. process data that might endanger the individual's physical health or safety in the event of a security breach.

6.3. Article 35 of the UK GDPR indicates that for personal data processing activities detailed in 6.2.1., 6.2.2. and 6.2.3. a DPIA is mandatory.

6.4. The Information Commissioner's Office (IC) establishes additional personal data processing activities – detailed in 6.2.4. to 6.2.13, which also requires a DPIA.

6.5. If the answer is ‘No’ to any question listed in 6.2.1. to 6.2.13. then a full DPIA will not be undertaken, but data protection advice will be sought from the DPO when required throughout the project’s lifecycle.

6.6. In some circumstances however, a DPIA will be undertaken even when the School has answered ‘No’ to all screening questions, especially when the project, or flows of personal data is complex as it is considered good practice to do so.

6.7. If the answer is ‘Yes’ to any question listed in 6.2.1. to 6.2.13. then a full DPIA will be undertaken.

6.8. The School will carry out a DPIA before implementing a new system or project, taking a ‘data protection by design and default’ approach to the processing of personal data.

7. What information should be included within a DPIA?

7.1. In line with Article 35 of the UK GDPR, the School will include:

7.1.1. A systematic description of the envisaged processing operations and the purposes of the processing (what the School will be doing with personal data);

7.1.2. An assessment of the necessity and proportionality of the processing operations in relation to the purposes (the School will assess whether there are alternative, less-intrusive ways to achieve the purpose that has been set out);

7.1.3. An assessment of the risks to the rights and freedoms of data subjects (the School will identify the potential risks to all individuals whose personal data is being processed);

7.1.4. The measures envisaged to address the risks (this will include safeguards, security measures etc. to ensure the protection of personal data).

7.2. The School will also ensure that all DPIAs will indicate which lawful basis under Article 6 of the UK GDPR is being relied upon to process the personal data.

7.3. When the DPIA identifies that special category personal data will be processed, the School will indicate which condition of Article 9 of the UK GDPR is being relied upon to process that data.

7.4. Within the DPIA, the School will also highlight:

7.4.1. Which data protection rights found under Articles 12 to 24 of the UK GDPR will or will not be affected;

7.4.2. Whether security measures are in place if the processing of personal data relates to a new application or computer system;
7.4.3. The retention periods of the personal data;
7.4.4. Whether data subject groups have been consulted with.

8. Completing a DPIA:

8.1. All completed screening question answers will be sent to the DPO for consultation.

8.2. All full DPIAs will be sent to the DPO for consultation.

8.3. The DPO will provide guidance and assistance during the development of a DPIA, and will submit their formal advice on the DPIA, but will not be required to provide a 'sign-off' to the DPIA and to the processing of personal data, since that is a decision of the controller itself.

8.4. The School considers a DPIA to be a 'living, breathing' document which means that should any new information come to light, the DPIA will be updated or reviewed to reflect that as soon as possible.

9. Complaints:

9.1. The School will manage a complaint made by a or on behalf of a data subject in compliance with the School's complaints policy. Complaints made in regard of the Schools management of personal data will be discussed with the DPO who will advise the School accordingly.

10. Contacts:

10.1. If you have any enquires in relation to this policy, please contact Claire Jones, Headteacher.

10.2. Further advice and information is available from the Information Commissioner's Office, Home / ICO or telephone 0303 123 1113 or 029 2044 8400 for the Wales Regional Office.

10.3. For further information relating to data protection principles and data subject rights please see the School's Data Protection Policy.

11. Review:

11.1. This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the DPO, Headteacher, or nominated representative.