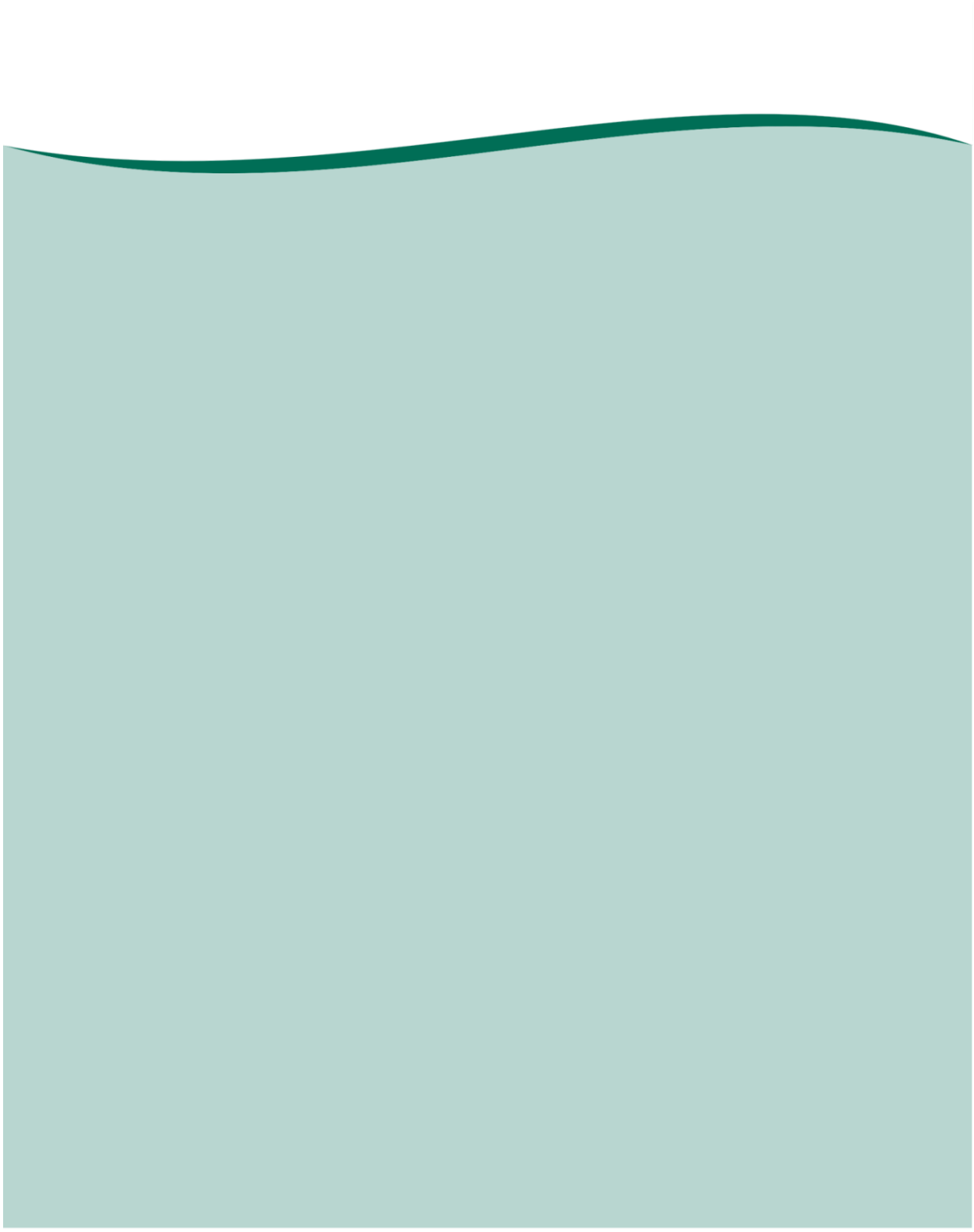
Data Protection Impact Assessment Policy



Document Control

Reference Number	Version 2.0	Status Approved	Sponsor(s)/Author(s) Andrew Holyoake, Data Protection Officer
Amendments	Updated to reflect GDPR		
Document objectives: To provide a framework for a formal assessment to ensure that new processes introduced meet privacy, confidentiality and data protection requirements			
Intended Recipients: Wiltshire Council Officers			
Group/Persons Consulted: None			
Monitoring Arrangements and Indicators: None			
Training/Resource Implications:			

Approving Body and Date Approved	IG Board
Date of Issue	Version 2 - April 2018
Review Date	April 2020
Contact for Review	Data Protection Officer, Information Governance
SIRO signature	

Associated Documentation:

Policies

- Data Protection Policy
- Information Asset Change Policy/Process

Legal framework

- Article 35 General Data Protection Regulation 2016
- Data Protection Act 2018

1 Introduction

1.1 This policy documentation sets out the organisation's Data Protection Impact Assessment Policy (DPIA).

1.2 This policy lays the framework for a formal assessment to ensure that new processes introduced meet privacy, confidentiality and data protection requirements.

1.3 Data Protection Impact Assessments are a tool which can help identify the most effective way to comply with data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow the organisation to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

2 Scope

2.1 This policy applies to all departments and functions of the organisation.

2.2 Adherence should be observed by all staff, contractors and partner organisations working on behalf of the organisation that introduce new processes or systems that are likely to involve a new use or significant change to the way in which personal data is handled.

3 Objective

3.1 All new project, processes and systems (including software and hardware) which are introduced must comply with confidentiality, privacy and data protection requirements. Therefore, before new processes or systems are introduced, they must be tested against these requirements.

3.2 To test against these requirements the organisation uses a Data Protection Impact Assessment.

4 Background to Data Protection Impact Assessments

4.1 **What Are DPIAs?** DPIAs are structured assessments of the potential impact on privacy for new or significantly changed processes. The DPIA should form part of the overall risk assessment of the process or project.

4.2 A DPIA helps the organisation to:

- Anticipate and address the likely impacts.
- Identify privacy risks to individuals.
- Foresee problems.
- Negotiate solutions.
- Protect the organisation's reputation.
- Offer assurance to stakeholders

4.3 **When Should a DPIA Be Undertaken?** Not every new project or changed process will require a DPIA. However, Article 35 of the General Data Protection Regulation 2016 (GDPR) requires that a DPIA be conducted where processing activity is likely to result in a high risk to the rights and freedoms of natural persons.

4.4 All projects using personal data, or projects making notable changes to the processing of personal data must be assessed against the DPIA screening questions to identify if a DPIA is required.

4.5 The Information Commissioner's Office (ICO) recommends that DPIAs are used wherever personal confidential data will be used or any other activity where the privacy of individual's data may be affected.

4.6 DPIAs are most effective when they are started at an early stage of the project or introduction of a process. Usually this is at the design or initiation stage, and ideally before any systems have been procured.

4.7 **Who Should Conduct a DPIA?** DPIAs should be conducted by someone that is introducing a new project or significantly changed process that involves personal data. The responsibility for carrying out the DPIA should be formally recorded and assigned, and it is ultimately the responsibility of the information asset owner to ensure completion.

4.8 **What Happens to a Completed DPIA?** DPIAs should be reviewed by the appropriate Project Board, and submitted to the Information Governance Manger and Data Protection Officer for comment and advice.

4.9 As a standing agenda item, a summary of DPIAs should be presented to the Information Governance Board.

4.10 DPIAs should form part of official Project Documentation where applicable.

5 Data Protection Impact Assessments

5.1 Article 25 of GDPR sets standards which require that data privacy is built into the working practices and structures of data controllers under the concept of protection by design and default therefore the Council needs to be able to demonstrate that all new or significantly changed processes or projects that involve personal data that are planned to be introduced comply with confidentiality, privacy and data protection requirements.

5.2 The purpose of the DPIA is to highlight to the organisation any privacy risks associated with a project. The key deliverable of a DPIA is a report that details impacts identified and the solutions or actions that will deal with them.

5.3 Conducting a DPIA is now a legal requirement when relevant, under Article 35 of the General Data Protection Regulation 2016.

5.4 Conventional project management techniques should be applied to the process of assessing privacy impact.

5.5 The DPIA should be started early in to the project life so that privacy risks are identified and appreciated before they are implemented into the project design. It is suggested that the DPIA should be commenced as part of a project's initiation stage.

5.6 Privacy implications should be considered at each phase of the life-cycle of a project.

5.7 The DPIA should be conducted by members of the project team, with a strong understanding of the project or process itself. With appropriate subject matter specialist support as required.

5.8 The outcomes of the DPIA should be:

a) The identification of the project's privacy impacts;

b) Appreciation of those impacts from the perspectives of all stakeholders;

c) An understanding of the acceptability of the project and its features by the organisations and people that will be affected by it;

d) Identification and assessment of less privacy-invasive alternatives;

e) Identification of ways in which negative impacts on privacy can be avoided;

f) Identification of ways to lessen negative impacts on privacy;

g) Where negative impacts on privacy are unavoidable, clarity as to the business need that justifies them; and

h) Documentation and publication of the outcomes.

6 DPIA Process

6.1 The Information Commissioners guidance for DPIAs sets out 9 steps which should be included in any DPIA undertaken. These steps are explained at Appendix 2

6.2 In order to decide if an Impact Assessment is required for a Project, the Screening Questions must be answered first.

7 Equality Impact Assessment

7.1 Equality Impact Assessments should be conducted on any policy that may have an impact on equality. The council has separate Equality and Inclusion guidance that relates to any council policy/activity, not just information related activities

8 Monitoring and Review

8.1 This policy will be reviewed once every two years by the IG Group. Auditing of this document should be done at least every two years based on monitoring the effectiveness of the policy in line with legislation and guidelines.

9 Appendix 1: General Data Protection Regulation 2016 - Principles

a) Personal data shall be processed fairly and in a transparent manner. (Transparency)

b) Personal data shall only be obtained only for specified explicit and legitimate purposes. (Purpose limitation)

c) Personal data shall be adequate, relevant and limited to what is necessary for the purpose. (Data minimisation)

d) Personal data shall be accurate and, where necessary, kept up to date, including necessary correction or erasure without delay. (Accuracy)

e) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary in a form that permits identification. (Storage limitation)

f) Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. (Integrity and Confidentiality)

9.2 In addition to the above the data controller – Wiltshire Council, shall be responsible for, and be able to demonstrate compliance with the above principles.

9.3 Personal data shall be processed in accordance with the rights of data subjects under the GDPR which include the following:

a) Right to access information held.

b) Right to rectification of inaccurate data or completion of incomplete data.

c) Right to erasure in certain circumstances.

d) Right to restrict processing of personal data.

e) Right to data portability.

f) Right to object to processing.

10 Appendix 2 - DPIA Stages

10.1 The following section is taken from the Information Commissioners DPIA Code of Practice (pages 12-14)

10.2 **A DPIA should incorporate the following steps:**

a) Identify the need for a DPIA

b) Describe the information flows

c) Identify the privacy and related risks

d) Identify and evaluate the privacy solutions

e) Sign off and record the DPIA outcomes

f) Integrate the outcomes into the project plan

g) Consult with internal and external stakeholders as needed throughout the process

10.3 **Identifying the need for a DPIA:**

a) Answer screening questions to identify a proposal's potential impact on privacy.

b) Begin to think about how project management activity can address privacy issues.

c) Start discussing privacy issues with stakeholders.

10.4 DPIAs should be conducted early during the project planning stage. The process will describe the overall aims of the project. The project development process should adapt to address privacy concerns.

10.5 **Describing information flows:**

a) Explain how information will be obtained, used, and retained – there may be several options to consider. This step can be based on, or form part of, a wider project plan.

b) This process can help to identify potential 'function creep' - unforeseen or unintended uses of the data (for example data sharing).

10.6 People who will be using the information are consulted on the practical implications. Potential future uses of information are identified, even if they are not immediately necessary.

10.7 **Identifying privacy and related risks:**

a) Record the risks to individuals, including possible intrusions on privacy where appropriate.

b) Assess the corporate risks, including regulatory action, reputational damage, and loss of public trust.

c) Conduct a compliance check against the Data Protection Act and other relevant legislation.

d) Maintain a record of the identified risks.

e) The process helps an organisation to understand the likelihood and severity of privacy risks.

f) An organisation is open with itself about risks and potential changes to a project.

10.8 **Identifying and evaluating privacy solutions:**

a) Devise ways to reduce or eliminate privacy risks.

b) Assess the costs and benefits of each approach, looking at the impact on privacy and the effect on the project outcomes.

c) Refer back to the privacy risk register until satisfied with the overall privacy impact.

10.9 The process should take into account the aims of the project and the impact on privacy.

10.10 The process will also record privacy risks which have been accepted as necessary for the project to continue.

10.11 **Signing off and recording the DPIA outcomes:**

a) Obtain appropriate signoff within the organisation within the project at Board level.

b) Produce a DPIA report, drawing on material produced earlier during the DPIA.

c) Consider publishing the report or other relevant information about the process.

10.12 The DPIA should be approved at a level appropriate to the project.

10.13 A DPIA report or summary should be made available to the appropriate stakeholders.

10.14 **Integrating the DPIA outcomes back into the project plan:**

a) Ensure that the steps recommended by the DPIA are implemented.

b) Continue to use the DPIA throughout the project lifecycle when appropriate.

c) Audit privacy impact solutions during and after project implemented

10.15 The implementation of privacy solutions is carried out and recorded.

10.16 The DPIA is referred to if the project is reviewed or expanded in the future.

11 Appendix 3 – Overview of the DPIA process

11.1 Identifying the need for a DPIA

a) The need for a DPIA can be identified as part of an organisation's usual project management process, or by using the screening questions.

11.2 Describing the information flows

a) Describe the information flows of the project. Explain what information is used, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information

11.3 Identifying the privacy and related risks

a) Some will be risks to individuals - for example damage caused by inaccurate data or a security breach, or upset caused by an unnecessary intrusion on privacy.

b) Some risks will be to the organisation - for example damage to reputation, or the financial costs or a data breach.

c) Legal compliance risks include the GDPR, PECR, and the Human Rights Act.

11.4 Identifying and evaluating privacy solutions

a) Explain how you could address each risk. Some might be eliminated altogether.

b) Other risks might be reduced. Most projects will require you to accept some level of risk, and will have some impact on privacy.

c) Evaluate the likely costs and benefits of each approach. Think about the available resources, and the need to deliver a project which is still effective.

11.5 Signing off and recording the DPIA outcomes

a) Make sure that the privacy risks have been signed-off at an appropriate level. This can be done as part of the wider project approval.

b) A DPIA report should summarise the process, and the steps taken to reduce the risks to privacy. It should also record the decisions taken to eliminate, mitigate, or accept the identified risks.

c) Publishing a DPIA report will improve transparency and accountability, and lets individuals learn more about how your project affects them.

11.6 Integrating the DPIA outcomes back into the project plan

a) The DPIA findings and actions should be integrated with the project plan. It might be necessary to return to the PIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process.

b) A DPIA might generate actions which will continue after the assessment has finished, so you should ensure that these are monitored.

c) Record what you can learn from the DPIA for future projects.

Appendix 4 – DPIA Screening Questions

a) Will the project involve the collection of new information about individuals?

b) Will the project compel individuals to provide information about themselves?

c) Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

d) Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

e) Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

f) Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?

g) 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 would consider to be particularly private.

h) Will the project require you to contact individuals in ways which they may find intrusive?

12 Appendix 5 - Examples of DPIA Projects

12.1 The Information Commissioners Office gives the following examples of where a DPIA might be necessary:

a) A new IT system for storing and accessing personal data.

b) A data sharing initiative where two or more organisations seek to pool or link sets of personal data.

c) A proposal to identify people in a particular group or demographic and initiate a course of action.

d) Using existing data for a new and unexpected or more intrusive purpose.

e) A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding Automatic number plate recognition capabilities to existing CCTV).

f) A new database which consolidates information held by separate parts of an organisation.

g) Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.