



Data Protection by Design Policy

Contents:

		Page
1	Introduction	2
2	Purpose	2
3	Objectives	3
4	Process	3
5	Procedures connected to this Policy	5
6.0	Links to Relevant Legislation	5
6.1	Links to Relevant National Standards	6
6.2	Links to other Key Policies	6
7	References	6
8	Roles and Responsibilities for this Policy	6
9	Training	7
10	Data Protection and Freedom of Information	7
11	Monitoring this Policy is Working in Practice	7
12	Guidance on the completion of - Data Protection Impact Assessment	8
13	Information Governance	9
14	Approval	9

Explanation of terms used in this policy:

Personal Data – information/data that identifies an individual.

Data protection impact assessment (DPIA) - is a process to help identify and minimise the data protection risks of a project. It is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of accountability obligations under the GDPR, and when done properly helps assess and demonstrate how YPAS complies with all data protection obligations.

Procedural Documents - the collective term for policies, procedures or guidelines

Project – for the purposes of this document a ‘project’ covers any: - change in process - formal project - changes or updates in IT Systems (including Security)

Policy - sets out the aims and principles under which services will operate. A policy outlines roles and responsibilities, defines the scope of the subject covered, and provides a high-level description of the controls that must be in place to ensure compliance.

1.0 Introduction:

Data Protection by design is a concept where Data Protection is considered as a core aspect of a project or change management process which promotes privacy and data protection compliance from the start. The Data Protection Impact Assessment (DPIA) is a mandatory tool as part of the data protection by design process.

This approach ensures that privacy and data protection is a key consideration in the early stages of any project and then throughout its lifecycle. For example, when:

- building new IT systems for storing or accessing personal data
- developing policy or strategies that have privacy implications
- embarking on a data sharing initiative
- using or collecting data for new purposes.

It is vitally important to ensure that as we progress with new and/or shared processes, services, and systems that the implementation does not result in an

adverse impact on information quality or a breach of information security, confidentiality, or data protection requirements. In particular the confidentiality, integrity, and accessibility of personal information must be maintained, and such information must be processed safely and securely.

2.0 Purpose:

This Policy sets out the mandatory elements of Data Protection by Design. The data protection by design approach is an essential tool in minimising privacy risks and building trust.

Designing projects, processes, products or systems with data protection in mind at the outset can lead to:

- Identifying potential problems at an early stage, when addressing them will often be simpler and less costly.

- Increased awareness of privacy and data protection concerns within the project
- Able to meet their legal requirements which leads to a reduced chance in any Data Protection breaches.
- The project will not be stalled at a later point when producing information sharing protocols/agreements.

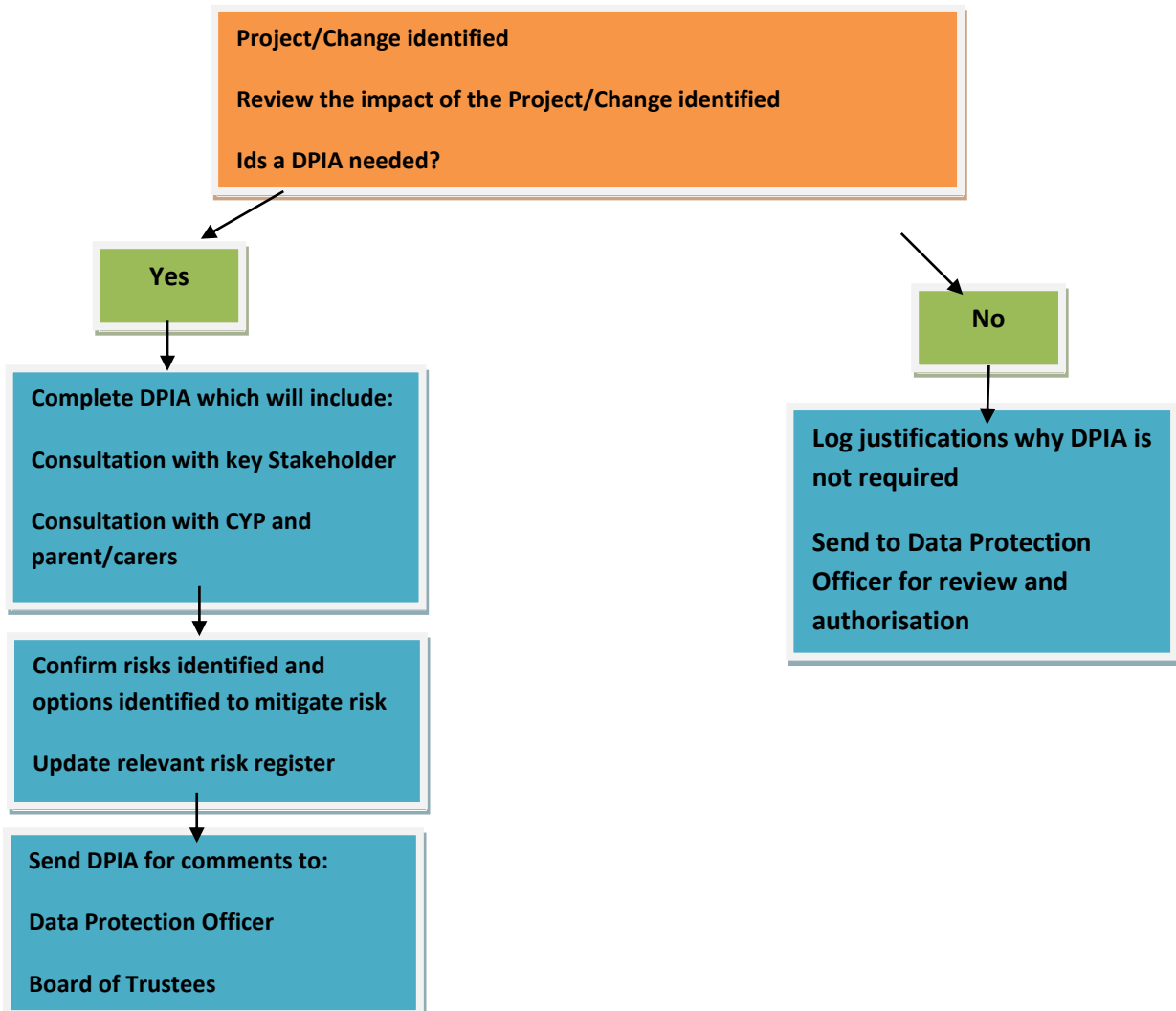
The use of the Data Protection Impact Assessment is mandatory according to relevant Data Protection legislation (General Data Protection Regulation). Non-compliance in relation to the use of the Data Protection Impact Assessment could lead to YPAS undergoing enforcement actions from the Information Commissioner which includes fines of up to 2% of the annual turnover.

3.0 Objectives:

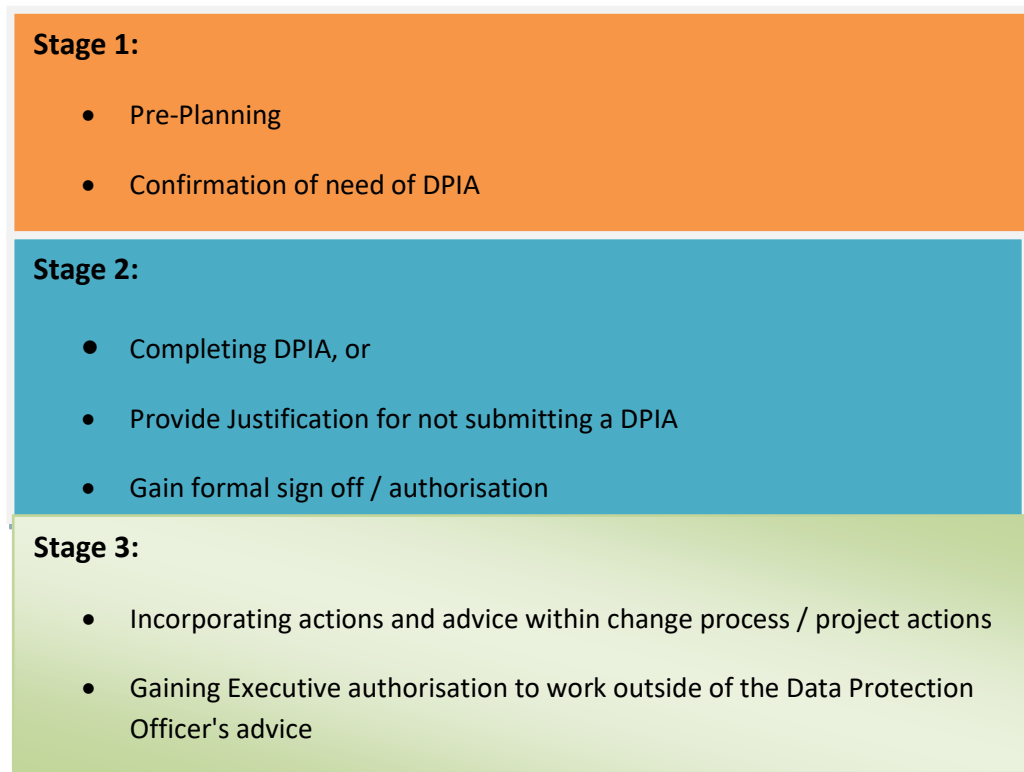
- To provide a step-by-step approach of how to integrate data protection by design within change management and/or project processes.
- To provide a Data Protection Impact Assessment tool for all staff to utilize

4.0 Process:

Data protection by design is formulated around the use of the Data Protection Impact Assessment. The below flowchart shows the process that must be followed in relation to Data Protection by Design:



The above flowchart identifies three key stages:



Stage 1:

There has been the following identified: - The need for a change in the collection, use and/or storage of data. - The need to undergo a project which could potentially affect data.

This triggers the need to consider the use of the data protection impact assessment (DPIA). Such considerations must be completed prior to the completion of any associated action planning. The DPIA must be completed if the change or project.

- The change in data processing is likely to result in a high risk (including some specified types of processing). - There may be an impact on any of an individuals' rights and freedoms, including (but not limited to) privacy rights.

Where it is agreed that a DPIA must be completed in full this must be integrated within the initial actions linked to the project/change.

Stage 2:

Where it is agreed that a DPIA the justification for this must be sent to the Data Protection Officer to review and confirm that there is no need to complete a DPIA.

Where it is identified that the DPIA is required all areas of the DPIA must be completed. There are six sections to the DPIA.

All risks identified within the DPIA must be included within a relevant risk register (where available). If there is no current risk raised linked to the project, then the project must be added to the risk register.

Stage 3:

Incorporating actions and advice within change process / project actions

Gaining Executive authorisation to work outside of the Data Protection Officer's advice

Once completed the DPIA must be sent to the Data Protection Officer and the Information Governance Steering Group for review and comments. The Information Governance Steering Group will provide their collective advice and comments against each requirement and any actions that they have identified. The Data Protection Officer will review each section of the DPIA, provide advice, comments and any actions required against each requirement. The Data Protection Officer will also authorise the DPIA; if authorised the project can continue, if the DPIA is not authorised the project must be reviewed in line with the Data Protection Officers overall comments.

Where the project will need to progress, but high risks have been identified within the DPIA the Data Protection Officer must notify the Information Commissioner of the project.

Stage 3 Where the DPIA has been completed, approved and Data Protection Officer's actions and advice are being adhered to: - Incorporate identified actions from the DPIA into the project action plans. - Agree frequency of updates to the Information Governance Steering Groups; the frequency of updates must be linked to the developments and timescales linked to the project.

Where a DPIA has been completed, approved and the Data Protection Officer's actions and advice are not being followed the following actions are required: - Document the justification for not following the Data Protection Officer's comments. - Present the completed DPIA along with the justification for not adhering to the Data Protection Officer's action to the Executive Management Team for formal Executive approval.

Where a DPIA has not been completed but it has been advised to complete a DPIA by the Data Protection Officer: - Document the justification for not following the Data Protection Officer's advice. - Present the Data Protection Officer's advice along with the justification for not adhering to the advice to the Executive Management Team for formal Executive approval.

Where it was agreed by the Data Protection Officer that a DPIA was not required the project documentation must provide evidence that the DPIA had been considered.

5.0 Procedures connected to this Policy:

- Risk Management Policy
- Information Governance Policy
- Information Sharing Policy

6.0 Links to Relevant Legislation:

General Data Protection Regulation (GDPR): The GDPR is the EU General Data Protection Regulation which will replace the Data Protection Act 1998 in the UK and the equivalent legislation across the EU Member States. The GDPR provides a legal framework for the processing of personal and special category data. The use of Data Protection Impact Assessments is mandatory under the General Data Protection Regulation.

6.1 Links to Relevant National Standards Data:

Protection Act General Data Protection Regulation 2017

6.2 Links to other Key Policies:

- Risk Management Policy
- Information Governance Policy
- Information Sharing Policy

7.0 References:

Article 29 Working Group; Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679

Information Commissioner Guidance via the ICO website

General Data Protection Regulation

8.0 Roles and Responsibilities for this Policy:

Title	Role	Key Responsibility
Data Protection Officer	Lead Authoriser of DIPA	To review the DPIA and ensure the validity of the information provided Provide advice and actions based on the information provided Authorise DPIA Monitor the DPIA
Data Protection Officer	Monitor	Monitor compliance with this policy Monitor DIPA
CEO and Trustees	Review and approve	Review and approve parts of procedure

9.0 Training:

What aspect(s) of this policy will require staff training?	Which staff groups require this training?	How will the training be delivered?	Who will deliver the training?	How often will staff require training	Who will ensure and monitor that staff have this training?
Completion of the Data Protection Impact Assessment	Any staff member who needs to complete a DPIA	Small group inductions	Data Protection Officer	Annually (Refresh)	Line managers

10.0 Data Protection and Freedom of Information:

Data Protection Act provides controls for the way information is handled and to gives legal rights to individuals in relation to the use of their data. It sets out strict rules for people who use or store data about individuals and gives rights to those people whose data has been collected. The law applies to all personal data held including electronic and manual records. The Information Commissioner's Office has powers to enforce the Data Protection Act and can do this through the use of compulsory audits, warrants, notices and monetary penalties which can be up to €20million or 4% of the Trusts annual turnover for serious breaches of the Data Protection Act. In addition to this the Information Commissioner can limit or stop data processing activities where there has been a serious breach of the Act and there remains a risk to the data.

The Freedom of Information Act provides public access to information held by public authorities. The main principle behind freedom of information legislation is that people have a right to know about the activities of public authorities, unless there is a good reason for them not to. The Freedom of Information Act applies to corporate data and personal data generally cannot be released under this Act.

All staff members have a responsibility to ensure that they do not disclose information about the Trust's activities; this includes information about service users in its care, staff members and corporate documentation to unauthorised individuals. This responsibility applies whether you are currently employed or after your employment ends and in certain aspects of your personal life e.g. use of social networking sites etc. The Trust seeks to ensure a high level of transparency in all its business activities but reserves the right not to disclose information where relevant legislation applies. The Information Governance Team provides a central point for release of information under Data Protection and Freedom of Information following formal requests for information; any queries about the disclosure of information can be forwarded to the Information Governance Team.

11.0 Monitoring this Policy is Working in Practice

What key elements will be monitored? (measurable policy objectives)	Where described in policy?	How will they be monitored ? (method + sample size)	Who will undertake this monitoring?	How Frequently?	Board that will receive and review results	Board to ensure actions are completed	Evidence this has happened
---	----------------------------	---	-------------------------------------	-----------------	--	---------------------------------------	----------------------------

12.0 Guidance on the completion of - Data Protection Impact Assessment:

Section	Information required	Where information can be obtained from	Support available for completion
Project overview	<p>Details about the change/project.</p> <p>Aims of the project/change.</p> <p>Who will be involved within the project?</p> <p>Is data affected by the proje</p>	<p>Project Initiation Documents.</p> <p>Change management information.</p> <p>Quality Impact Assessments</p>	<p>Project Manager</p> <p>Project Management Office</p> <p>Information Governance Team</p> <p>Data</p>
Data Processing	<p>Details about the use of data including what you will be: - Obtaining - Using - Sharing - Storing - Deleting</p> <p>Details showing the differences between what we do currently and what are intended.</p> <p>The reasons for any changes</p>	<p>Risk register</p> <p>Project Initiation Documents.</p> <p>Change management information.</p> <p>Quality Impact Assessments</p>	<p>Project Manager</p> <p>Project Management Office</p> <p>Information Governance Team</p> <p>Data</p>
Proportionality	<p>A review of what is proposed to see if the use of the data is lawful and if there are alternatives to the approach.</p>	<p>General Data Protection Regulation</p> <p>Asset Register</p>	
Consultation process	<p>Evidence of what consultation has taken place to complete the DPIA and what consultation is planned as part of the project</p>		
Corporate Data	<p>Confirmation of the creation of new corporate documentation.</p> <p>Confirming business continuity arrangements for the project and for the change once implemented</p>		

Risks	To identify and confirm the risks associated with the project, including any new risks which arise from the change linked to the DPIA	Risk Register	
Approval and Review	Documented audit trail of the reviews and approvals of the DPIA.		

13.0 Information Governance:

Personal identifying Information concerning clients or staff is strictly confidential and must not be disclosed to unauthorised persons. This obligation shall continue in perpetuity. Disclosures of confidential information or disclosures of any data of a personal nature can result in prosecution for an offence under the General Data Protection Regulations 2018 or an action for civil damages under the same Act in addition to any disciplinary action taken by the YPAS.


14.0 Approval:

Policies and Procedures are approved by YPAS's Chief Executive Officer and Ratified by the Board of Trustees.

Policy approved by:

Monique Collier (Chief Executive Officer).

Signature:



Date: 17/08/2022