

Data Protection by Design Policy

CONTENTS:

Number	Description	Page
1	Introduction	Page 2
2	Purpose	Page 2
3	Objectives	Page 2
4	When DPIA is Required	Page 2
5	DPIA Process	Page 3
6	Roles and Responsibilities	Page 4
7	Training	Page 5
8	Information Governance	Page 8
9	Approval	Page 8

1. Introduction:

YPAS is committed to ensuring that privacy and data protection are embedded into all projects, processes, and systems from the outset. This approach, known as Data Protection by Design, ensures compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and protects the rights and freedoms of individuals.

A key element of this approach is the Data Protection Impact Assessment (DPIA), which must be carried out whenever a project or change is likely to involve high-risk processing of personal data.

2. Purpose:

This policy sets out how YPAS applies Data Protection by Design to ensure that:

- Data protection is considered at the earliest stages of planning new projects, services, or processes.
- DPIAs are completed whenever data processing activities present risks to privacy.
- Risks are identified early and mitigated effectively.
- YPAS complies with its legal obligations and maintains the trust of service users, staff, and stakeholders.

3. Objectives:

- To provide a clear step-by-step process for integrating Data Protection by Design.
- To ensure accountability and compliance with UK GDPR and the Data Protection Act 2018.
- To promote a culture of privacy and information security across YPAS.

4. When DPIA is Required:

A DPIA must be completed when a project or change involves processing that is likely to result in a high risk to individuals. Examples include:

- Introducing new IT systems that collect, store, or share personal data.
- Making significant changes to existing systems or processes.
- Developing policies, strategies, or services that have privacy implications.
- Establishing new data sharing arrangements with partner organisations.

Where uncertainty exists, consultation should take place with the Data Protection Officer (DPO) to confirm whether a DPIA is required.

5. DPIA Process:

There are 2 distinct routes to managing Absence and Performance:

Identify: At project initiation, consider whether personal data will be affected.

Consult: Seek advice from the DPO to decide whether a DPIA is required.

Assess: Complete the DPIA, identifying risks and mitigation measures.

Review: Submit the DPIA to the DPO and the Information Governance Steering Group for review and approval.

Implement: Integrate agreed actions into project planning and risk registers.

Escalate: Where high risks remain, the DPO may be required to notify the ICO before the project proceeds.

If the DPO advises a DPIA is not required, the decision and rationale must be documented. Where advice is not followed, justification must be presented to senior management for approval.

6. Roles and Responsibilities:

- Data Protection Officer (DPO): Reviews and authorises DPIAs, provides advice, monitors compliance, and escalates to the ICO where necessary.
- CEO and Trustees: Approve projects where residual risks remain and oversee compliance with this policy.
- Project Leads / Managers: Ensure DPIAs are completed where required and that risks are managed and recorded.
- All Staff: Must consider data protection implications in their work and comply with DPIA processes where relevant.

7. Training:

Staff involved in projects, change management, or data processing must receive training on Data Protection by Design and DPIA requirements. Refresher training will be provided annually, led by the DPO.

8. 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 Data Protection Act 1998 or an action for civil damages under the same Act in addition to any disciplinary action taken by the YPAS.

9. Approval:

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

Name: Monique Collier (*Chief Executive Officer*).

Signature: 

Date: 28/08/25