Data Protection by Design and Default Policy and Procedure

This policy and procedure sets out how Southend-on-Sea City Council will imbed a culture of privacy by design in the way it conducts its business.

Whenever a piece of work starts which involves using information about people (their personal data) we will look at the risks which may be associated.

We will always make sure that the data protection core principles are met. This will usually be through a Data Protection Compliance Check.

For matters that, if not properly addressed, might involve a serious risk to privacy, we will carry out a Data Protection Impact Assessment.

As early as possible in any project or proposal, the officer responsible for a plan or project should complete the Initial Data Protection Risk Assessment form so that the proportionate action regarding data protection can be identified.

There is no need to delay if plans are not initially fully formed as the process is most helpful if it can inform projects at an early stage.

Plans may need to be delayed or halted completely if data protection matters are not fully risk assessed and sign-off obtained.

Author: Valerie Smith
Version: 5
Review/Revision date: April 2027

1. Introduction

This policy applies to anyone responsible for the delivery or management of a project or business process, or the letting or management of a contract or similar arrangement, where the proposed activity will involve the processing of personal data.

This policy will apply where new technology is being introduced; that is, any proposal for the purchase of hardware, software, third party or cloud hosted services. It will also apply to proposals which involve the processing of personal data on databases, websites, mobiles and other Apps.

Under data protection legislation we have an obligation to make thinking about how we protect people's personal data an integral part of the way in which we conduct our business.

How personal information will be looked after needs to be considered at the start of a process; developed along with the project and then monitored once it transfers to business as usual.

The aim of this policy is to identify and minimise privacy risks while still meeting required business aims.

This policy is to be applied before procurement activity starts, irrespective of the value of the procurement and including proposals with nil cost.

2. Help and support

The Data Protection Risk Support Service can provide support with the consideration of data protection risks. ICT can provide support with cyber security risks, and technological data protection matters such as data in transit and data at rest. ICT will also advise on system rationalisation. This will avoid the duplication of assets, ensure technological benefits to the project and the wider organisation are identified and maximised. They will also assess whether ongoing support for any new system will be supplied by ICT.

3. When should a data protection risk assessment take place?

The data protection risk assessment should start early on, following conception of a project or proposal, so that the results can be built into the wider project plan. Risk assessment and risk mitigation will evolve throughout the project until its final completion.

4. What sort of activity requires a data protection risk assessment?

Cost is not a factor; the relevant consideration is whether a proposal involves the processing of personal data. If personal data is to be used to any extent, the proper use and safeguarding of that data needs to be considered.

This is likely to include, but is not limited to, the purchase of hardware and software, the letting of contracts with a third-party provider and changes in the way information is used or managed.

5. Initial Data Protection Risk Assessment

The first step is to complete an Initial Data Protection Risk Assessment (IDPRA). This will include a brief explanation of the matter being considered, the type and scale of personal data to be processed and the type of technology to be used (if appropriate).

The IDPRA will be considered by the Data Protection Risk Support Service, alongside ICT where there are cyber security considerations.

In discussion with the proposer, a rating of high, medium or low data protection risk will then be allocated. This will determine the level of data protection assurance that will be required.

Advice will be provided about likely data protection risks. Identified risks should be transferred into the risk register for the project plan, where this exists.

It is important that the IDPRA is completed as early as possible as some data protection requirements (such as the location of data storage or the capability to delete data) are non-negotiable and can mean that a project must be abandoned or amended, regardless of the work which has gone on up to that point.

The Information Asset Register will be updated by the Data Protection Risk Support service to reflect the new or amended use of personal data.

6. Low and Medium Risk Processing (Data Protection Compliance Check - DPCC)

In instances where the processing of personal data is minimal, the IDPRA may be sufficient. More often, proposers of low or medium risk projects will be advised to follow the Data Protection Compliance Check (DPCC) process.

This consists of a checklist of matters the proposer will need to address in order to properly safeguard and manage the personal data they will be collecting.

It provides assurance that data has sufficient safeguards and is being collected, used and stored in accordance with data protection principles. Its complexity will vary depending on the data and systems involved. This will ensure all relevant data protection risks and requirements have been considered.

Once complete, the Data Protection Compliance Check will be signed off by the Data Protection Risk Support Service. It will be attached to the Information Asset Register as evidence of compliance.

The proposal may not become operational until identified data protection and ICT issues have been resolved.

7. High Risk Processing (Data Protection Impact Assessment - DPIA)

Proposers of high risk projects will be advised to complete a formal Data Protection Impact Assessment (DPIA). This provides for a more in depth look at the application of

data protection and cyber security requirements, the associated risks and how they may be mitigated.

It is important to be able to demonstrate that high risk processing has had sufficient safeguards applied to minimise any risk.

Failure to do so could result in senior management or the Information Commissioner vetoing the processing.

High risk processing is likely to be where there is a significant change in the way in which personal information is used. This is likely to be where:

- The project or proposal has a wide scope
- It uses new or intrusive technologies
- Particularly sensitive or high risk data or individuals are involved
- Information was collected for one purpose but is now intended to be used for another.

This is likely to apply where the proposer is:

- Implementing a new or unusual type of technology
- Implementing new monitoring, surveillance or testing procedures
- Using special category (sensitive) personal data, or the scope of personal data increases
- Consolidating information held by separate parts of our organisation
- Using personal data already held for a new purpose
- Acting in relation to a new grouping or demographic of identified individuals
- Sharing personal data, or pooling or linking data with additional organisations

Successful completion of the Data Protection Impact Assessment will involve a team or people with a range of expertise and skills. Important features are:

- An understanding of the project's aims and the organisation's culture
- Authority to influence the design and development of the project and participate in decisions
- Expertise in privacy and compliance matters
- Expertise in technology, processes and activities relevant to the project
- Expertise in the Council's digital strategy
- Ability to assess and communicate organisational risks
- Ability to assess which privacy solutions are feasible for the relevant project
- Ability to communicate effectively with stakeholders and management (such as those who have existing customer relationships).

Data Protection legislation requires the advice of the Data Protection Officer to be sought when carrying out a DPIA.

Depending on the nature of the data processing and the aims and ambitions of the proposal the Data Protection Risk Support Service and ICT will work with the proposer to identify how the data protection risk process will be managed. This will then need to be built into the project's plans.

Once Data Protection and strategic fit risks have been managed to the satisfaction of the Data Protection Risk Support Service and ICT, the DPIA will be referred to either the SIRO or Caldicott Guardian for final sign off, or will be signed off by the Data Protection Risk Support Service. The appropriate sign off will be determined by the Data Protection Risk Support Service, based on the residual level of risk.

As Data Protection Impact Assessments are reserved for high unmitigated risk proposals, it is essential that sufficient time is allowed for proper consideration to take place.

The proposal may not become operational until any identified data protection issues have been resolved.

8. Ownership of Data Protection Risk

While the Data Protection Officer (through the Data Protection Risk Support Service) and ICT will advise on data protection legislation, compliance and risk mitigation, ultimately the risk belongs to the service area concerned. They must satisfy themselves that they have sufficiently identified and considered risks in relation to data protection.

9. Confirmation of Compliance in Principle

Once the Data Protection Risk Support Service and ICT are assured that data protection requirements have been sufficiently considered, each will confirm compliance in principle. This will enable any associated procurement and financial process to go ahead.

10. Throughout the project

It is unlikely that at the outset of a project or proposal all the required information will be to hand. The Data Protection Risk Support Service and ICT will work with lead officers throughout the project to ensure data protection requirements are met.

Support can also be provided by the Data Protection Risk Support Service with Privacy Notices and Data Sharing Agreements.

It is particularly important during procurement that tender evaluation questionnaires contain sufficient pass/fail questions relating to data protection and that any eventual contracts contain the mandatory data protection clauses and description of permitted data processing. Advice can be sought regarding this from the Procurement service, supported by the Data Protection Risk Support Service where required.

Version Control

Date	Version	Reason	Owner	Author
May 2018	V1	Compliance with GDPR and replacement of document Business Processes/Project Management Guidance – Privacy Impact Assessment	Val Smith	Val Smith
January 2020	V2	Minor wording change. References to the Smart City Agenda updated to reflect current ICT priorities. IDPRA being sufficient in some instances recognised. Sign off for DPIA corrected from Privacy Officer to SIRO. Reference to certificate of compliance removed. IDPRA template removed	Val Smith	Val Smith
May 2022	V3	Minor wording change, expanded explanation of DPIA sign off, reflection of City status	Val Smith	Val Smith
May 2023	V4	Reviewed and updated to reflect rebrand and current information governance structure	Val Smith	Karen Finn
April 2025	V5	Biennial review and update to Governance	Val Smith	Karen Finn

Purpose:	To embed data protection by design at an early stage in planning processes.
Status:	Final Version
Date of Revision	April 2025
To be reviewed by:	April 2027
Governance:	Corporate Leadership Team