

Data Protection Impact Assessment Guidance

The Information Commissioner's Office (ICO) defines a Data Protection Impact Assessment (DPIA) as: 'a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. They help identify privacy risks, foresee problems and bring forward solutions.'

What is a Data Protection Impact Assessment?

A DPIA is a process that assists organisations in identifying and minimising the privacy risks of new projects or policies. It will help to ensure that potential problems are identified at an early stage when addressing them will often be simpler and less costly. Conducting a DPIA should benefit the Council by producing better policies and systems, and improving the relationship with individuals.

Why should I carry out a DPIA?

Whilst not a legal requirement, it is often the most effective way to demonstrate to the ICO how personal data processing complies with the General Data Protection Regulations (GDPR). A project or service which has been subject to a DPIA should be less privacy intrusive and therefore less likely to affect individuals in a negative way. A DPIA should improve transparency and make it easier for individuals to understand how and why their information is being used.

When should I carry out a DPIA?

The core principles of a DPIA can be applied to any project or service that involves the use of personal data, or to any other activity that could have an impact on the privacy of individuals. Answering the screening questions in Stage 1 of the DPIA should help you identify whether there are privacy matters that need addressing.

Who should carry out a DPIA?

Responsibility for conducting a DPIA are best placed at Managers Forum level.

How do I carry out a DPIA?

The requirement for a DPIA will be identified by answering the questions in Stage 1. If a requirement has been identified, you should complete all the relevant sections in Stage 2. The Data Protection Officer (DPO) will review the DPIA and will confirm whether the proposed measures address the privacy risks identified and could potentially make recommendations for additional measures needed.

All DPIAs have to be emailed for checking before a decision is made (i.e. before the report is sent to Corporate Management Team and the Executive Board). Therefore, please send your report and impact assessment to informationgovernance@n-kesteven.gov.uk at least 5 working days before the first report deadline. The DPO commits to providing comments within 4 working days.

If you are unsure if a DPIA is required, please contact the DPO as early as possible.