Cheltenham Borough Council Data Protection Impact Assessment Policy

Version control

Document name: Data Protection Impact Assessment Policy

Version: 1.0

Responsible officer

- Claire Hughes, Corporate Director and Monitoring Officer

Approved by: Cabinet

Next review date: May 2026

Retention period: Delete one year after new version

Revision history

Revision date	Version	Description
May 2023	1	New Policy

Consultees

Internal

- Corporate Governance Group and Leadership Team

External

- N/A

Distribution

All Staff and Council Website

Contents

1. Introduction and purpose of the policy

1.1. Conducting a Data Protection Impact Assessment (DPIA) is a legal requirement for any type of processing, including certain specified types of processing that are likely to result in a high risk to the rights and freedoms of individuals.

1.2. Cheltenham Borough Council (the Council) is committed to using people's personal data properly and legally, to ensure it is used only in ways people would reasonably expect and that it stays safe. Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we collect, store and process personal data about our citizens, service users, employees, suppliers and other third parties. We recognise that the correct and lawful treatment of this data maintains trust and confidence in the organisation and provides for successful service delivery.

1.3. This policy sets out the Council's obligations to undertake a DPIA where any processing of personal data is 'likely to result in a high risk to the rights and freedoms of individuals', as set out in Articles 35 and 36 of the UK GDPR and section 64 of the DPA 2018.

1.4. It provides the details on when a DPIA is required, the responsibility of completing a DPIA and also the implications regarding the failure to carry out a DPIA to the organisation.

1.5. Employees of the Council are obliged to comply with data protection laws when processing personal data on our behalf. A breach of the data protection laws may result in criminal proceedings and may result in disciplinary action which could result in dismissal.

1.6. Data Processors acting on the instructions of the Council are obliged to comply with this policy when processing personal data on our behalf, as detailed in the contract between the Council and the processor.

1.7. The policy should be read and complied with in conjunction with our Data Protection Policy

2. What is a DPIA and how to undertake them

2.1. A Data Protection Impact Assessment is a written assessment which helps the Council identify, evaluate, and mitigate risks and privacy impacts to data subjects arising as a result of processing their personal data.

2.2. An effective DPIA allows us to identify and fix problems at an early stage, bringing broader benefits for both individuals and our organisation.

2.3. A DPIA must be undertaken before the processing of any personal data which is 'likely to result in a high risk to the rights and freedoms' of data subjects or to where processing is of a large scale, involves automatic decision-making including profiling or monitoring which decides on access to services and opportunities or involves sensitive data or vulnerable individuals or where data matching across various datasets is carried out. The ICO provides details on when a DPIA must be undertaken in their guidance: ICO guidance. They also provide a template.

2.4. High risk activity examples may include:

- Anything that has an automated component that can deny someone a service (financial applications, credit check etc)
- Large scale profiling of individuals
- Biometric – workplace entry systems, facial recognition, fingerprint access controls
- Data Matching – fraud prevention, personal usage of statutory services or benefits
- Invisible processing – re-use of publicly available data
- Tracking – employee location data, lone workers devices, tracing services

2.5. A DPIA ensures compliance with data protection legislation and other legal and regulatory requirements. It helps to:

- identify privacy risks to individuals
- anticipate and address the likely impacts
- foresee problems and find solutions
- protect our reputation and offer assurance to stakeholders.

2.6. Responsibility for carrying out the DPIA process sits with the Project Manager who should ensure that the need for a DPIA is assessed and that a DPIA is completed if required. This assessment and completion should be done at the outline business case stage of a project or before a change to existing processing activities.

2.7. The completed DPIA should form part of the project risk assessment and official project documentation.

3. Conclusion

3.1. The DPIA process is a fundamental part of our compliance with data protection laws. If you need further assistance please consult the ICO website: www.ico.org.uk or contact the data protection officer Data.Protection@cheltenham.gov.uk