Data Protection Policy

Document Overview

This policy is in place to ensure members of staff are aware of their responsibilities and outlines how Kirklees Council complies with the core principles of the UK General Data Protection Regulation (UKGDPR) and the Data Protection Act (DPA). This will be achieved by ensuring:

- Compliance with data protection legislation, guidance and best practice.
- Openness and transparency as to how personal data is stored and processed.
- Risks to information are identified and mitigated against to protect against the risks of a data breach.

Intended Audience

All Kirklees employees, Elected Members (Councillors), volunteers and organisations working on behalf of Kirklees

Linked Policy

- Information Governance Policy
- Information Security Policy
- Information Sharing and Processing Policy
- Records Management Policy
- Licencing the Reuse of Council Information Policy
- Freedom of Information Policy

Revision History

Version	Author	Reason for issue	Date
6.0	Katy Deacon	Reviewed Policy	13/05/21
7.0	Erin Wood	Reviewed Policy	July 2023

Date of next revision
November 2026

1. Introduction
Kirklees Council is required to process (hold, obtain, record, use, share) certain information about residents and members of staff (in any capacity) in accordance with its legal obligations under the UK General Data Protection Regulation (UKGDPR), Data Protection Act (DPA), and other relevant legislation.

2. Policy Scope
This policy applies to all departments and functions within Kirklees Council and those working on behalf of the Council including, but not limited to, Councillors, contractors, agency workers, volunteers and work experience placements.
This policy outlines the behaviours and responsibilities expected to ensure the council continues to fulfil its obligations under the UKGDPR, the DPA and related Data Protection legislation.

3. Data Protection
Kirklees Council needs to process personal data to deliver its services efficiently and effectively. The Council will use personal data in the most efficient and effective way possible to deliver better services and enhance privacy.
All staff and individuals who have access to Council data are responsible for complying with this policy and data protection legislation, ensuring good information governance practices are always followed.

4.1 Applicable data
Personal data refers to any information relating to a living person (a 'data subject') who can be identified directly or indirectly, including pseudonymised data and special category data.
Anonymised or aggregated data is not regulated by the legislation, providing that the anonymisation or aggregation has not been done in a reversable way.

This policy is applied to both digital and manual records and filing systems.

4.2 Principles
Kirklees Council fully support the data protection principles and will process personal data in accordance with the requirements outlined in data protection legislation:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

Where the Council processes personal data as a 'competent authority' for 'law enforcement purposes' (i.e., under statutory law enforcement functions), it shall do so in accordance with the version of the data protection principles set out in the Law Enforcement provisions of the Data Protection Act. Those principles are similar (but not identical) to those outlined above.

4.3 Data protection by design

Kirklees Council's approach to compliance with data protection legislation will be underpinned by the principles of data protection by design and default.

Data protection by design ensures that consideration is given to privacy and data protection issues in the design phase of any system, service, product, or process, continuing to evaluate this throughout the lifecycle of the project.

Data protection by default ensures that only the data that is needed to achieve your specific purpose is processed. This embeds the fundamental data protection principles 'data minimisation' and 'purpose limitation'.

4.4 Individuals' rights

Data protection legislation provides individuals with various rights:

1. The right to be informed,
2. The right of access,
3. The right of rectification,
4. The right to be forgotten,
5. The right to restrict processing,
6. The right of data portability,
7. The right to object,
8. Rights related to automated decision making, including profiling.

The rules relating to individual rights are different where the Council processes personal data as a 'competent authority' for 'law enforcement' purposes.

The Council is required to respond to all information rights requests without undue delay and within one calendar month from the date of receipt. In some instances, where the case is complex, the deadline may be extended by to up to three months. Where a request is made in relation to processing for 'law enforcement purposes', there is not an option to extend beyond one month.

4.5 Lawful processing

The Council processes personal data for many reasons, including in relation to the services it provides and in its role as an employer. In most instances, the Council will be the data controller (usually alone, but sometimes jointly) in respect of the personal data it processes; on occasion it may act as a data processor on behalf of another data controller.

Whether acting as a data controller or a data processor, the Council will maintain a record of its processing activities. Information concerning the processing of personal data in respect of which the Council is a data controller will be communicated by the Council to data subjects by means of appropriate privacy notices.

The Council will ensure that its processing of personal data (other than law enforcement processing) fulfils the appropriate general condition(s) for processing outlined in the UKGDPR.
Where a 'special category' of personal data is processed, the Council will ensure that one of the additional conditions set out in relation to special categories of personal data in the UKGDPR is also met, along with any further requirements

regarding the processing of sensitive personal data set out in other Data Protection legislation.

Similar conditions apply to personal data relating to criminal convictions and offences. When processing such data, the Council will ensure that the relevant additional conditions and requirements are met.
Where the Council processes personal data as a 'competent authority' for 'law enforcement purposes' it shall do so in accordance with the requirements of the law enforcement provisions of the Data Protection Act.

4.6 Privacy Notices
Kirklees Council will always make available a suitable and up to date privacy notice for data subjects.
Service privacy notices will also be made available for specific processing activities.
A privacy statement will always be provided to data subjects where they provide their personal data, sign posting to the appropriate privacy information.

4.7 Data security
Kirklees Council will process personal data in accordance with the appropriate security policies. To ensure the security of personal data, the Council has appropriate physical, technological, and organisational measures in place. This includes ensuring that appropriate access controls are in place (only those with a business need can access the information) and that appropriate levels of access are granted. Access controls and permissions should be reviewed regularly.

4.8 Data sharing
Information must only be shared on a need-to-know basis and where there is a lawful reason for sharing – internally and externally.

Any sharing of Council controlled personal data with other data controllers must comply with all statutory requirements and corporate policies. Where appropriate, the Council will enter into a data or information sharing agreement (DSA/ISA) before sharing any personal data.

Any sharing Council controlled data with a data processor, appropriate contracts must be in place, including a data processing agreement (DPA) before sharing any personal data.

4.9 International transfers
Data protection regulations vary across different countries and regions and adequate protections must be in place. There are strict rules regarding the transfer of personal data to other countries. Kirklees Council will not transfer personal data outside of the UK without having the appropriate contractual, security and privacy arrangements in place.

4.10 Video surveillance (including CCTV)
Kirklees Council is dedicated to responsible and lawful use of surveillance camera systems whilst safeguarding the privacy and data protection rights of individuals. By adhering to the principles set out in the Surveillance Camera Code of Practice, ICO CCTV Code of Practice, and relevant data protection legislation, the Council will maintain transparency, accountability, and public trust in its surveillance activities.

4.11 Data breaches

Kirklees Council will ensure that all staff handling personal data know when and how to report any actual or suspected data breach. The Information Governance Team will ensure that the breach is managed correctly, lawfully and in a timely manner. Breaches will be reported to the ICO by the Information Governance Team where necessary.

4.12 Retention and Destruction

Personal data must only be held for as long as necessary for the purposes of the processing activity. Each service maintains a retention schedule that is specific and relevant to the specific types of information processed by the service.
Personal data must be destroyed securely and in a way that protects the rights and privacy of the data subject.

5. Education and training

All members of staff will undertake mandatory data security awareness training annually. Training and guidance materials will be provided and updated by the Information Governance Team.

6. Monitoring Compliance and Effectiveness

The DPO and Information Governance Team will conduct regular audits to monitor compliance with this policy. Compliance and effectiveness will also be monitored by the Information Governance Board.

7. Associated Documents / Further Reading

This policy should be read in conjunction with all other Information Governance related policies and procedures. Further guidance is available on the intranet.