Data Protection Policy

Sheffield City Council processes personal data on a daily basis. Data protection law requires the Council, its employees and authorised users, to process personal data fairly, lawfully and securely at all times. This policy sets out the key activities and responsibilities the Council need to adhere to.

14 May 2019 **Release** Version 2.1

Document Review

Title	Name(s) / Board	Role / Responsibility
Policy owner	Mark Gannon	Director Business Change and Information Solutions
Change requests to	Mark Jones	Senior Information Management Officer
Key stakeholder review	Information Governance Working Group	Portfolio representatives to contribute and implement information governance policy, procedures and best practice
	General Data Protection Regulations (GDPR) Working Group	Portfolio representatives to ensure procedures align with new data protection requirements with GDPR and the Data Protection Act 2018

Document approval

Authorising Body	Date of acceptance
Information Governance Board	08th June 2018
Local Negotiating Committee	14th May 2019
HR Policy Forum	22nd May 2019

Version History

Version	Issue Date	Comments / Summary of changes
1.0	12/06/2014	Policy to replace the Handling Personal Information Policy (2002). Policy added to Officers' Code of Conduct (Appendix G) in July 2015
1.1-1.3	18/04/2018, 25/05/2018	Policy review and refresh for General Data Protection Regulations (GDPR) and Data Protection Act (2018)
2.0	08/06/2018	Minor change following IGB comments
2.1	14/05/2019	Minor change following LNC re. training refresh times

Review

Review Date	June 30th 2020

1. Introduction and Definitions

Sheffield City Council processes personal data to carry out its duties to make decisions and provide public services. Personal data is defined in law, but in essence it is information that identifies a living person (the subject of the data) or can make them more identifiable.

"***Personal data***" includes, but is not exclusive to: name, address, date of birth, email address, telephone number, unique reference numbers (e.g. NHS number, National Insurance number, Vehicle Registration Number), financial details (e.g. bank details, transactions, arrears, etc.).

Personal data also includes "***Special Category Data***", which is sensitive personal data, covering for example: ethnicity, religious beliefs, political opinions, sexuality, physical and mental health conditions, genetic and biometric data, as well as data of criminal offences and convictions.

The term "***processing***" is also defined in law and refers to any operations involving personal data such as collection, recording, organisation, storage, alteration, retrieval, consultation, use, disclosure, combination, erasure or destruction.

All the personal data processed for or on behalf of the City Council must be processed in accordance with data protection law: the European Union's General Data Protection Regulations and the UK's Data Protection Act that both came into effect on May 25th 2018.

The intention of this policy is to identify the key principles, activities and responsibilities that all our employees have to adhere to as well as all the people who are authorised to process personal data to carry out council business. For the purpose of this policy, ***authorised users*** includes Councillors, contractors, suppliers, agency workers, partnership workers (like NHS, police employees), and volunteers.

2. Policy Requirements

Data protection law sets out a number of key principles, so that the processing of personal data shall be:

1 ….Processed ***fairly, transparently*** and ***lawfully***

2 … Processed ***only*** for specified and ***not incompatible purposes***

3 … ***Adequate***, ***relevant*** and ***necessary*** for the purpose

4… ***Accurate*** and, where necessary, ***kept up-to-date***

5 … Not kept ***longer*** than ***necessary*** for the purpose

6 ….Keep ***secure*** by ***technical***/***organisational*** means

7 ….and the Council should demonstrate compliance (***Accountability***)

Further obligations and rights in the "*Applied GDPR*"

- all ***Data Subjects' rights*** are subject to ICO enforcement
- Transfer personal data outside EEA only if ***privacy*** protected

To comply with the above principles, the City Council will

- Register as a Data Controller with the Information Commissioner's Office (Data Protection Register – No. Z6548192) and register the details of the Council's Data Protection Officer.
- Undertake Data Privacy Impact Assessments where required and ensure sign off by the Data Protection Officer before new processing takes place.
- Follow the Code of Practices, recommendations and guidance produced by the Information Commissioner, as the UK's supervisory body, and the European Union Data Protection Board, to process personal data in line with the principles above (e.g. Record of Processing Activities, Privacy by Design, Data Protection Impact Assessments, Retention Schedules, etc.).
- Ensure all employees have completed the Council's Information Management e-learning, or attended a taught course, and watched the Cyber Security training videos within the first six weeks of starting with the Council or their role that involves the processing of personal data.
- Employees refresh their information management training every two years, unless they work in social care or public health whereby they are required to complete an annual refresh to support the NHS Digital Data Protection and Security Toolkit submission.
- Ensure all ***authorised users*** that process personal data have completed the same training as Council employees, unless they can prove they have completed the equivalent training at their respective organisations in the last 6 months.
- Write and publish appropriate privacy notices to make it clear what personal data we need to process, the reasons why, whether collecting the data is optional or not, and what we intend to do with the data (storage, retention, sharing).
- Maintain an Information Asset Register to support the Record of Processing Activity (ROPA's).
- Tell people if we have to share their personal data with other 3rd parties to deliver a service and, if necessary, record if consent is needed and has been given, refused or withdrawn
- Inform people of their rights to request access to the personal data we hold about them, and their rights to ask for their data to be corrected or deleted or the processing restricted, and to act upon those requests promptly and within the agreed timescales.

- Only collect the personal data we need, the minimum necessary.
- Only use personal data for the purposes for which it was collected, unless it can be used without contravening the law (e.g. using anonymised or pseudonymised data, historical research and statistics, crime detection and prevention, etc.).
- Take all reasonable steps to secure the personal data being processed and to apply controls to support access on a need to know basis.
- Retain personal data for only as long as we need to and to delete or destroy personal data in a timely and secure manner in line with the Council's Document and Records Management Policy and Retention Schedule.
- Ensure contractual clauses, data processing agreements and information sharing agreements are in place when Council information is being shared or processed by external third parties.
- To log and investigate all reported personal data breaches and to notify the Information Commissioner within the statutory timescales and the affected data subjects accordingly in line with the Council's Information Security Incident Standard Operating Procedure.

3. Policy Implementation

Employees and authorised users are responsible for their actions when handling personal data.

Heads of Service (or their equivalent) are responsible for ensuring the relevant processes and procedures are in place within their service areas and are followed when personal data is processed.

Directors to address any information governance issues identified in the Annual Governance Statement (Section I).

Executive Directors to ensure their Portfolio complies with this policy.

4. Data Protection Officer

The Data Protection Officer role is a legal requirement to monitor internal compliance, inform and advise an organisation's of its data protection obligations, provide advice on Data Protection Impact Assessments and to act as a contact point for data subjects and the supervisory authority (the Information Commissioner's Office).

The Council's Data Protection Officer is currently Mark Jones, Business Change and Information Solutions, and can be contacted by email at DataProtectionOfficer@sheffield.gov.uk

5. Compliance

Failure to comply with data protection law can have significant consequences and could affect the health and well-being of the individuals whose data is being processed, the reputation of the Council potentially resulting in public mistrust, fines, legal action and lost business opportunities.

All employees and authorised users are expected to adhere to the principles of this policy and data protection law in general, and where there is a suspicion or evidence to the contrary, disciplinary proceedings may be taken.

This page is intentionally left blank