General Data Protection Regulations

Version	Date of Adoption	Minute Reference	Review Date	Originator
2020-v1	17.3.2020	123-2020	March 2020	K Dewey/G White
2021	25.3.2021	97-2021	March 2021	K Dewey/G White
2022-03	24.3.2022	97-2022	March 2023	K Dewey/G White
2022-03	21.3.2023	130-2023	March 2024	K Dewey/G White

General Data Protection Regulations

1. Introduction

1.1 Scope

This policy describes how we protect individual's privacy when processing their data, and how we comply with associated data protection law, regulation and good practice.

For further information, comments or suggestions, please contact:

Keith Dewey – Data Protection Advisor

DPA@datagrc.co.uk

+44(0) 208 133 0242

1.2 Compliance

Compliance with this policy is mandatory for all staff and councillors. Failure to comply with this policy or failure to notify the full council/DPA of breaches may result in disciplinary and legal action. The council will use reasonable means to monitor compliance with this policy.

If an exception is required to this policy, formal approval must be gained in advance from the Full Council.

1.3 Terms

Data Subjects	The individual identified by Personal Data, including residents, councillors, volunteers and staff.
Personal Data	Any data relating to an identified or identifiable living individual. This covers any media, it includes electronic, digital, hardcopy, paper and audio.
Processing	Any handling of data including collation, transfer, access, alteration, storage or deletion.
Sensitive Data	Higher risk Personal Data, which has a great possibility of being used for fraud or creating distress to the individual, such as "Special Data", criminal convictions and personal identity documents.
Special Data	Data relating to race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life, and sexual orientation.
Staff	Refers to anyone working or acting on behalf of the council, or who is processing personal data obtained for the council's use, including employees, contractors, consultants and third-party agents.

Contents

2. Key Roles

2.1 All Staff and Councillors

(a) Responsible for complying with this policy, relevant legislation and guidance.

2.2 Full Council

(a) Ultimately responsible for ensuring that the council meets its legal and ethical obligations.

2.3 Data Protection Advisor

(a) Keeping the full council updated about data protection obligations, responsibilities, risk and issues.

(b) Reviewing data protection policies and procedures.

(c) Arranging data protection training and advice for staff and councillors (online training module available).

(d) Handling data protection questions from staff and the full council.

(e) Reviewing Data Protection Impact Assessments (DPIAs).

(f) Monitoring compliance with this policy.

(g) Overseeing requests from Data Subjects.

(h) Engaging with the Information Commissioner's Office (ICO) where required.

2.4 Full Council

(a) Overseeing the compliance of processes and services the council manages.

3. Mandates

3.1 General

(a) We comply with **relevant legislation and regulations**.

(b) We provide staff and councillors with the **opportunity of training** on the requirements of this Policy.

(c) We **escalate queries or concerns** to the full council or to the Data Protection Advisor.

(d) We make a copy of this policy **available to all staff and councillors** and it is **freely available on our website.**

(e) We maintain procedures to detail **how to comply** with policy requirements.

(f) We maintain central records of our significant **privacy risks and decisions**.

3.2 Before Collecting Data

(a) We document processes that use personal data in our Records of Processing.

(b) We manage data privacy risks throughout the **design and development lifecycle**.

(c) We identify and comply with the **lawful basis** for that process, as one of:

(i) Vital Interest
(ii) Legal Obligation
(iii) Public Task
(iv) Contract
(v) Consent
(vi) an exemption granted under law with formal DPA approval
(vii) specific conditions granted under law for the processing of special categories of data with formal DPA approval

(d) We perform a **Data Privacy Impact Assessment** (DPIA) if there is a potential risk to a Data Subject.

(e) We identify how long data will be **retained** for, based on the service, purpose or legal requirement, and how we will delete it.

(f) We design **secure processes** to handle the data.

(g) We design processes that minimise the processing of that data to that required for the business purpose **(privacy by default).**

(h) We identify any potential **international transfers** of the data and ensure adequate safeguards are deployed.

3.3 Before using Third Parties for Processing

(a) We formally agree **contracts** that include the GDPR contractual requirements.

(b) We conduct **due diligence** to verify contractors have adequate privacy and security controls.

(c) We understand who the third party will be sharing the data with **(supply chain)** and verify that their controls appear adequate.

3.4 When Collecting Data

(a) We only capture data that is **absolutely necessary** for specific business processes.

(b) We let the Data Subject know what we plan to do with their data through clear and **approved Privacy Notices.**

(c) We **layer** Privacy Notices to improve readability, so that Data Subjects are initially presented with high level information but can follow links to additional details.

(d) We ensure any required **consent** is:

(i) **Freely given** with balance of power. Not a precondition of a service.

(ii) **Clear**, separate from terms and conditions, and transparent.

(iii) **Specific and granular**.

(iv) Gained through **clear affirmation action**.

(v) As **easy to opt-out** as it was to opt-in.

(vi) Approved by an **authorised guardian** if the Data Subject using our online services is below 14 years of age.

(vii) **Recorded** as evidence.

(e) We seek to, in a timely manner, notify the Data Subject if we have **indirectly obtained** their data.

(f) We notify the Data Subject of any **website Cookies** being used.

(i) We allow Data Subjects to **opt out from Cookies** that are not necessary for the performance of the website.

(ii) We provide **Cookie Notices** to provide full transparency of their use of data.

3.5 When Using Data

(a) We only use personal data in a **fair, transparent and lawful manner**.

(b) We only use the data in accordance with the **secure process** that was approved.

(c) We take reasonable steps to **maintain the accuracy** of data, based on its business purpose, especially when inaccuracies are identified or when notified by the Data Subject.

(d) We **securely delete or anonymise** data that is no longer needed or has reached the end of its retention period.

(e) We only **duplicate data** if that replication is unavoidable to achieve the business purpose.

(f) We perform **on going monitoring** of the processing across our council and Processors.

3.6 When Marketing Data Subjects

(a) We ensure **specific consent** has been received before sending unsolicited electronic communications to individuals and Sole Traders.

(b) We remove any Data Subjects who have **opted out**.

(c) We remove any Data Subjects that are on relevant industry suppression files, such as the **Telephone Preference Service**.

3.7 When a Data Subject makes a Formal Request

(a) We follow **formal procedures** to receive, manage and respond within approved timescales.

(b) We **validate the identity** of the Data Subject before disclosing personal data.

(c) We **maintain the security** of the data throughout the process.

(d) We only respond with **messages that are authorised** by the Data Protection Advisor.

(e) We provide our responses **at no cost** to the Data Subject.

(f) We **redact personal data** belonging to other individuals where appropriate.

(g) We formally support data subjects' legal rights to request that we explain our processing of their data; provide them, or a third party nominated by the data subject with a copy of their data; and to correct, erase or restrict processing of their data.

(h) We immediately refer any requests from **law enforcement agencies** (e.g. Police) to the Data Protection Advisor.

(i) We respond to data subject requests within four weeks, unless an extension has been agreed with the DPA and the data subject has been notified.

Review: March 2024