Policy and Resources
Monday 21 July 2025

PART I

Data Management Policies
(ADCCC)

1 Summary

1.1 This covering report is submitted for consideration and approval of the attached policies:

- Data Protection Policy (update to existing policy)
- Privacy Policy (new)
- Subject Access Request (SAR) Policy (previously contained within the Data Protection Policy)
- Freedom of Information (FOIA) and Environmental Information Regulations (EIR) Policy (replaces current FOIA guidance for staff)
- Data Retention Policy (update to existing policy)
- Special Category Personal Data and Criminal Offence Data Policy (new)

1.2 These documents aim to ensure compliance with legal obligations, enhance transparency, and protect the rights of individuals regarding their personal data.

1.3 The attached policies collectively reinforce the council's commitment to data protection and transparency and are updated version of previous overarching Data Protection and Privacy policies.

1.4 The additional policies have been developed to provide Officers with more comprehensive guidance and a clear point of reference. These policies are designed to support Officers in effectively carrying out their responsibilities and to ensure that the Council fully complies with its legal and regulatory obligations. This includes responsibilities under Subject Access Requests (SARs), the Freedom of Information Act (FOIA), the Environmental Information Regulations (EIR), data retention requirements, and the handling of special category personal data.

1.5 Together they provide a framework for handling personal data responsibly and in compliance with the UK General Data Protection Regulation (UK GDPR), and the Data Protection Act 2018.

1.6 This report seeks approval for the adoption and implementation of these policies to ensure the council meets its statutory obligations and maintains public trust.

1.7 The initial draft documents were submitted to Sharpe Pritchard LLP for review and feedback. Following their review, the firm provided detailed comments and suggestions regarding various aspects of the documents. These comments were carefully considered and incorporated into the revised versions of the documents submitted with this report, including the creation of the standalone Special Category Personal Data and Criminal Offence Data Policy.

2 Recommendation

That:

2.1 The option detailed at 4.1 is selected.

2.2 The Committee agrees to give delegated Authority to Associate Director of Corporate, Customer and Community to authorise minor changes to the policy, such as terminology, clarification, or administrative corrections with no significant impact.

2.3 That public access to the report be immediate.

Report prepared by: Phil King (Data Protection and Resilience Manager)

3 Details

3.1 Data Protection Policy: Establishes the principles for collecting, processing, and storing personal data, ensuring compliance with relevant legislation and promoting data security within the council.

3.2 Privacy Policy: Describes how the council collects, uses, and protects personal data, ensuring that individuals are informed about their rights and the council's data practices.

3.3 Subject Access Request (SAR) Policy: Outlines the procedures for individuals to request access to their personal data held by the council, ensuring timely responses and adherence to the statutory timeframe.

3.4 Freedom of Information (FOI) and Environmental Information Regulations (EIR) Policy: Details how the council will respond to requests for information, balancing transparency with the need to protect sensitive information.

3.5 Data Retention Policy: Sets out the guidelines for retaining and disposing of data in compliance with legal requirements, thereby minimising risks associated with data retention.

3.6 Special Category Personal Data and Criminal Offence Data Policy: Defines the procedures for processing sensitive personal data, including health, racial, or criminal offence data, ensuring compliance with data protection laws such as UK GDPR. It outlines the legal basis for processing such data and implements robust security measures to protect against unauthorised access or misuse.

3.7 Separate procedures are available for staff to support them in complying with these policies

4 Options and Reasons for Recommendations

4.1 <u>Approve the Attached Policies as Presented.</u>

4.1.1 Ensures compliance with legal obligations and best practices in data protection.

4.1.2 Builds public trust and demonstrates the council’s commitment to safeguarding personal data.

4.2 <u>Approve the Policies with Amendments.</u>

4.2.1 Allows customisation to better fit the council's needs while still meeting legal requirements.

4.2.2 Risks delaying implementation and could create compliance gaps if amendments compromise core principles.

4.3 Reject the Policies.

4.3.1 Exposes the council to legal risks, including significant fines for non-compliance.

4.3.2 Undermines public confidence in the council's ability to manage personal data and could lead to inconsistent practices.

5 Policy/Budget Reference and Implications

5.1 The implementation of these policies aligns with the Council's Corporate objective to "*Provide responsive and responsible local leadership*".

5.2 There are no additional costs associated with training staff to comply with these policies so can be considered within the existing budget.

6 Financial Implications

6.1 The Information Commissioner's Office (ICO) can impose fines of up to £17.5m or 4% of annual global turnover (whichever is higher) for serious breaches of data protection laws. This could pose a significant financial risk for the council in the event of a data breach.

7 Legal Implications

7.1 Compliance with UK GDPR and the Data Protection Act 2018 is mandatory. Failure to implement these policies could result in legal action and financial penalties.

8 Equal Opportunities Implications

8.1 The policies ensure that all individuals are treated equally regarding access to their data and information, promoting fairness and inclusivity.

9 Staffing Implications

9.1 Staff training will be necessary to ensure understanding and compliance with the new policies.

9.2 No additional staffing resource is needed to comply with the policies.

10 Communications and Website Implications

10.1 The council's website will need to be updated to reflect the new policies, ensuring public access to information regarding data protection practices.

11 Risk and Health & Safety Implications

11.1 Implementation of these policies will help mitigate risks associated with data breaches, ensuring that the council has robust processes in place.

12 Environmental, Community Safety, Public Health and Customer Services Centre Implications

12.1 None specific.

APPENDICES / ATTACHMENTS

Data Protection Policy 2025 – 2028

Privacy Policy 2025 – 2028

Subject Access Request Policy 2025 – 2028

FOI and EIR 2025 – 2028

Data Retention Policy 2025 – 2028

Special Category Personal Data and Criminal Offence Data Policy 2025 – 2028