Appropriate Policy Document (APD) for the Processing of Special Category and Criminal Offence Data

This Policy Document explains the Council's processing of special category personal data (SC) and criminal offence (CO) data and its policies with regard to the retention and erasure of personal data processed in reliance on these conditions.

It satisfies the requirement of the Data Protection Act 2018 (DPA 18) Part 4 for a Data Controller (that is the Council) to have in place an 'appropriate policy document'. This should be read in conjunction with the Council's Data Protection Policy.

This Policy covers all processing carried out by the Council:

- which is subject to UK General Data Protection Regulation (GDPR) Articles 9 and 10
- in reliance of the conditions set out in the Data Protection Act 2018, Schedule 1: *Special categories of personal data and criminal convictions etc. data*, in particular:
    - Part 1 Conditions relating to employment, health and research etc.
    - Part 2 Substantial public interest conditions
    - Part 3 Additional conditions relating to criminal convictions etc.

When the Council carries out the processing of special categories of personal data a condition under UK GDPR Article 9 must be satisfied. The Council will do so with reference to the following:

- Paragraph 2(a) -the data subject has given explicit consent for one or more specified purposes
- Paragraph 2(b) - the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- Paragraph 2(g) - the processing is necessary for reasons of substantial public interest
- Paragraph 2(j) – the processing is necessary for archiving purposes in the public interest, scientific or historical research or statistical purposes in accordance with UK GDPR Article 89 (1)

Irrespective of whether the Policy is applicable, the Council must also be compliant with the principles relating to the processing of personal data. This Policy will complement our Record of Processing Activity (ROPA) as required under Article 30 GDPR and provides SC and CO data with further protection and accountability.

Description of data processed

DATA PROTECTION ACT SCHEDULE 1 PART 1

Conditions relating to **Employment, Social Security and Health etc**:

- For the purpose of carrying out our obligations as an employer in connection with our rights under employment law
- Processing data relating to criminal convictions under Article 10 UK GDPR in connection with our rights under employment law in connection with recruitment, discipline or dismissal
- Processing necessary for revenue and benefits and health or social care purposes

DATA PROTECTION ACT SCHEDULE 1 PART 2

Substantial Public Interest Conditions:

- Fulfilling the Council's obligations under UK legislation for the provision of services to residents within the Borough
- Complying with other legal requirements, such as the requirement to disclose information in connection with legal proceedings

Equality of opportunity:

- Processing necessary to ensure that the Council fulfils its public sector equality duty when carrying out its activities
- To ensure compliance with the Council's obligations under legislation such as the Equality Act 2010
- Ensuring equal access to all its services and to all sections of the community in recognition of its legal and ethical duties to represent and serve communities

Personal data processed under this category is limited to:

- Personal data revealing racial or ethnic origin
- Personal data revealing religious or philosophical beliefs
- Data concerning health
- Personal data concerning an individual's sexual orientation

Racial and ethnic diversity at senior levels of organisation:

- Applies only to the processing necessary to identify suitable individuals to hold senior positions within the Council due to substantial public interest

Preventing or detecting unlawful acts:

- Processing data concerning criminal records in connection with employment in order to reduce the risk to the Council and the local community
- Carrying out enforcement action in connection with the Council's statutory duties

Regulatory requirements relating to unlawful acts and dishonesty:

- Complying with the Council's enforcement obligations under UK legislation
- Assisting other authorities in connection with their regulatory requirements
- Processing data concerning dishonesty, malpractice, unfitness or other improper conduct in order to protect the local community
- Carrying out investigations and disciplinary actions relating to employees

Preventing fraud

- Processing necessary for the purposes of preventing fraud
- Disclosure or processing in accordance with arrangements made by an anti-fraud organisation

Counselling

- For the provision of counselling, advice or support or of another similar service provided confidentially

Safeguarding of children and individuals at risk

- Protecting vulnerable children and or an individual aged over 18 from neglect, physical, mental or emotional harm
- Sharing information with relevant agencies for the purposes of safeguarding

Safeguarding of economic well-being of certain individuals

- Protecting the economic wellbeing of an individual at economic risk who is aged 18 or over
- Identifying individuals at risk while attending emergency incidents
- Data sharing with our partners to assist them to support individuals

Insurance

- Claims for loss or damage to Council property
- Claims for compensation made against the Council by third parties

Occupational pensions

- Fulfilling the Council's obligation to provide an occupational pension scheme
- Determining the benefits payable to dependents of pension scheme members

Disclosure to elected representatives

- Assisting elected representatives such as local government Councillors and Members of Parliament with requests for assistance on behalf of their constituents

DATA PROTECTION ACT SCHEDULE 1 PART 3

Additional Conditions Relating to Criminal Convictions, etc.

Extension of conditions in Part 2 of Schedule 1 referring to substantial public interest.

- The Authority may process personal data where it is strictly necessary for law enforcement purposes and it meets the relevant conditions in the DPA 2018 Schedule 8 – paragraph 1 – statutory purposes

Procedures for ensuring compliance with the principles

Accountability principle

We have in place appropriate technical, security and organisational measures to demonstrate our accountability. These are overseen by the Council's Information Governance Strategic Board, chaired by the Senior Information Risk Owner.

They include:

- Taking a 'data protection by design and default' approach to our activities
- Implementing data protection and information security policies
- Carrying out Data Protection Impact Assessments (DPIAs) when the processing is likely to result in high risk to individuals
- Ensuring that we have written contracts in place with our data processors and data sharing agreements with our partners
- A designated Data Protection Officer with expert knowledge of data protection law and practices and the ability to fulfil tasks indicated in UK GDPR Article 39
- Maintaining a Record of our Processing Activities (ROPA) and Information Asset Registers (IARs)
- Keeping records of the mandatory data protection and information security training for all staff, carried out at least annually
- Undertaking regular data protection audits
- Maintaining logs of information security incidents, requests from data subjects exercising their rights and enquiries from Council officers and elected representatives
- Regularly reviewing our accountability measures using the ICO's Accountability Framework

Principle (a): lawfulness, fairness and transparency

As a local authority we are bound by statute. Our functions are set out in numerous Acts of Parliament and many of these functions have associated legal duties. We process SC/CO to comply with our obligations imposed by them.

We will ensure that:

- Personal data is only processed where a lawful basis applies
- Data subjects are provided with clear and transparent information about why we process their personal data in our privacy notices and this policy document

Principle (b): purpose limitation

We process SC/CO data to fulfil our statutory obligations in accordance with relevant legislation.

We will ensure that:

- The data we collect will be for specified, explicit and legitimate purposes
- Data subjects will be informed of those purposes in a Privacy Notice

- Personal data will not be processed for purposes incompatible with the original purpose it was collected for
- If we are sharing data with another controller we will have documented the legal basis for doing so

Principle (c): data minimisation

We will ensure that:

- The SC/CO data we collect is adequate, relevant and limited to what is necessary for the purpose for which it is processed
- SC/CO data is retained in accordance with the Council's Retention and Disposal Schedule
- We regularly remind employees to delete personal data no longer needed

Principle (d): accuracy

We will ensure that:

- SC/CO data shall be accurate and kept up to date. If we become aware it is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that the data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights do not apply, we will document our decision
- Requests from data subjects challenging the accuracy of data are sent to the appropriate department and we will document our decision
- The accuracy of personal data will be checked during audits

Principle (e): storage limitation

We will ensure that:

- SC/CO data is retained in accordance with the Council's Retention and Disposal Schedule unless we have identified the need to keep for public interest archiving, scientific or historical research, or statistical purposes
- The retention period is based on our legal obligations and business needs and reviewed regularly and updated when necessary
- We only keep personal data in identifiable form as long as is necessary for the purpose for which it is processed

Principle (f): integrity and confidentiality (security)

We will ensure that all SC/CO data is processed that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

These include:

- ISO 27001 accreditation, NHS Data Security Protection Toolkit, Payment Card Industry Standards
- Role-based access controls are implemented to restrict access to SC/CO data
- Encryption and other technical security controls to secure SC/CO data within systems, including the use of pseudonymisation

- Mandatory annual Data Protection and Information Security Training for all staff
- Acceptable use of IT equipment and systems defined in Information Security Management System Manual
- Identity and Access Management through Human Resources
- Strong defences of the Council's core IT system (e.g. Firewalls, Malware Detection & Defence)
- Encryption of Data in transit where appropriate
- The ability to monitor and / or log digital and user activity in Council systems where appropriate
- Deployment of Information Security Tools (e.g. Data Loss Prevention, Mobile Device Management, Secure External Email)
- Assurance of Council Technical Security Architecture by Independent 3rd party partners
- Annual and ad-hoc IT Health Checks and Penetration Tests by independent certified test teams; with follow-up treatment of identified vulnerabilities
- Robust procedures for the reporting of any data or potential data breaches.
- Regular audits of physical measures and office walkthroughs
- A suite of IG policies in place, which are reviewed on a biennial basis
- Full compliance with the Public Service Network (PSN)

Retention and erasure policies

SC/CO data is held and disposed of in line with Council's Record Retention and Disposal Schedules.
We will ensure that:

- our Information Asset Registers (IARs) are kept up to date and set out the ownership, governance and maintenance of the Council's assets
- when disposing of SC/CO information it is carried out securely
- we assess the right retention period for SC/CO data by considering the following:
  - the amount, nature, and sensitivity of the personal data
  - the potential risk of harm from unauthorised use or disclosure
  - the purposes for which we process the data and it can be achieved through other means
  - any legal or regulatory requirements

Other Documentation

This policy should be read in conjunction with:

- Data Protection Policy
- Records Management Policy
- Records Retention and Disposal Schedule
- Data Breach Guidance
- Privacy Notices

APD review date

The policy was approved by the Information Governance Strategic Board on 3 March 2021. It will be reviewed bi-annually, or more frequently if recommended by the Data Protection Officer.