Appropriate Policy Document

1. Introduction

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category data and criminal convictions and offence data under certain specified conditions.

This is the 'Appropriate Policy Document' for Newark and Sherwood District Council [the Council] that sets out how the Council will protect special category data and criminal convictions and offence personal data.

2. Scope

This Policy covers all processing carried out by the Council which is subject to UK General Data Protection Regulation (GDPR) Articles 9 (Processing of special categories of personal data) and 10 (Processing of personal data relating to criminal convictions and offences) and in reliance of the conditions set out in the Data Protection Act 2018, Schedule 1 (Conditions for processing special categories of personal data and criminal convictions data).

It describes how the Council is compliant when processing 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.

This Policy also covers all sensitive processing of personal data that falls within the scope of Law Enforcement which is subject to Part 3 of the Data Protection Act 2018, and which is separate from the UK GDPR regime.

3. Purpose

The purpose of this document is to explain:

- the Council's procedures which are in place to secure compliance with the data protection principles set out in Article 5 of the GDPR and Section 35-40 of the DPA 2018
- when the processing is carried out by the Council in reliance on one of the conditions set out in Schedule 1, Parts 1-3; and
- the Council's policies about the retention and erasure of such personal data processed in reliance on a condition specified in Schedule 1 of the DPA 2018.

4. Definition of special category, sensitive and criminal offence data

Special category data (defined by Article 9 of the UK General Data Protection Regulation (UK GDPR)) and sensitive data (defined by section 35 of the DPA 2018) is personal data which reveals:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person

- data concerning health
- data concerning a natural person's sex life or sexual orientation

In addition, the UK GDPR gives extra protection to "personal data relating to criminal convictions and offences or related security measures".

Section 11(2) of the DPA provides that references to personal data relating to criminal convictions and offences or related security measures include personal data relating to:

(a) the alleged commission of offences by the data subject, or
(b) proceedings for an offence committed or alleged to have been committed by the data subject, or the disposal of such proceedings, including sentencing.

Therefore any data that falls within this definition of criminal convictions and offences must also meet a condition in Part 1, 2 or 3 of Schedule 1.

5. Conditions for Processing Special Category Data and Criminal Conviction Data

Article 9: Special Category Data

Within the UK GDPR, all processing of special category data must meet an Article 9(2) condition in order for that processing to be lawful. The Article 9(2) conditions for processing special category data are:

Article 9(2)(a)	Explicit consent
Article 9(2)(b)	**Employment, social security and social protection**
Article 9(2)(c)	Vital interests
Article 9(2)(d)	Not-for-profit bodies
Article 9(2)(e)	Made public by the data subject
Article 9(2)(f)	Legal claims or judicial acts
Article 9(2)(g)	**Reasons of substantial public interest (with a basis in law)**
Article 9(2)(h)	**Health or social care (with a basis in law)**
Article 9(2)(i)	**Public health (with a basis in law)**
Article 9(2)(j)	**Archiving, research and statistics (with a basis in law)**

- If processing is reliant on conditions (b), (h), (i) or (j), an associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018 must be met.
- If processing is reliant on Article 9(2)(g) Reasons of substantial public interest, an associated condition in UK law, set out in Part 2 of Schedule 1 of the DPA 2018 must be met.

When the Council processes special category data, the majority of this processing is for the following permitted purposes in UK GDPR Articles 9:

Article 9(2)(b)	**Employment, social security and social protection**
The council processes special category data about our employees that is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, photographs and their membership of any trade union.	
Article 9(2)(g)	**Reasons of substantial public interest (with a basis in law)**
Processing for reasons of substantial public interest relates to the data we receive or obtain in order to fulfil our statutory function as a Local Authority. This includes information about our customers, tenants and service users. This may include information such as ethnicity, health and criminal convictions. For example in relation to housing needs, grants and revenue and benefits.	

The Council may also occasionally process some special category data in accordance with other Article 9 UK GDPR conditions, such as:

- 9(2)(a) 'explicit consent' – the Council may rely on explicit consent as the basis for processing. When it does, the Council ensures that explicit and freely given consent for each special category data item sought, that the data subject is informed they have the right to withdraw their consent at any time, and that processes are in place to easily facilitate the withdrawal of consent;
- 9(2)(c) 'vital interests' – the Council may rely on this condition under certain exceptional circumstances to protect an individual's vital interests;
- 9(2)(f) 'for the establishment, exercise or defence of legal claims'

These other Article 9 conditions do not require an associated condition in UK law as set out in Schedule 1 of the DPA 2018 and do not require mention in this Appropriate Policy Document. Nonetheless, the Council will always process any special category data in accordance with the Data Protection Principles as laid out in Section 11 of this Policy.

Article 10: Criminal Offence Data

To process criminal offence data the Council must be able to demonstrate:

- a lawful basis under Article 6; and
- either official authority or a Schedule 1 condition for processing criminal offence data under Article 10.

The main lawful basis for processing criminal convictions data is Article 6(e) processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Where the Council is processing criminal offence data for purposes other than Law Enforcement purposes and where it is not processing under the control of official authority, a Schedule 1, Part 3 condition is identified within this Appropriate Policy Document.

Where the Council is processing criminal offence data for Law Enforcement purposes and under the control of official authority, the Council will not be required to identify a Schedule 1 condition for processing. This processing is covered by Part 3 of the Data Protection Act 2018, and is separate from the UK GDPR regime.

6. Schedule 1 Conditions

PART 1: Conditions Relating to Employment, Social Security and Social Protection

As an employer there are various laws relating to employment and social protection that must be complied with, for instance, laws relating to parental leave, adoption leave, statutory leave, maternity pay, sick pay, unfair dismissal and laws promoting equality and diversity and preventing discrimination and harassment.

Where the council processes special category personal data under this condition, it shall only be used for the purposes of complying with legal obligations relating to employment or social protection laws, for example:

- 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

PART 2: Substantial Public Interest Conditions

Section 10 (2) of the DPA sets out that in order for processing of special category and criminal offence data to be necessary for the purposes in Article 9(2)(g) of the UK GDPR (reasons of substantial public interest), it must meet one of the conditions in Part 2 of Schedule 1 of the DPA.

These conditions must have a basis in law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The council processes special category data under the following Substantial Public Interest Conditions:

Statutory etc and government purposes
- Fulfilling the Council's obligations under UK legislation for the provision of services to residents within the district of Newark and Sherwood.
- Complying with other legal requirements, such as the requirement to disclose information in connection with legal proceedings.

Equality of opportunity or treatment
- Ensuring compliance with obligations under legislation such as the Equality Act 2010.
- Ensuring we provide equal access to our services, to all sections of the community in recognition of our legal and ethical duty to represent and serve communities.

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 community.
- Carrying out enforcement action in connection with the Council's statutory duties.

Protecting the public against dishonesty etc
- Processing data concerning dishonesty, malpractice or other improper conduct in order to protect the local community.
- Carrying out enforcement action in connection with the Council's statutory duties.
- Carrying out investigations and disciplinary actions relating to our employees.

Regulatory requirements relating to unlawful acts and dishonesty etc
- 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
- Disclosing personal data in accordance with arrangements made by an anti-fraud organisation.

Safeguarding of children and individuals at risk

- Protecting vulnerable children and young people from neglect, physical, mental or emotional harm.
- Identifying individuals at risk while attending emergency incidents.
- Obtaining further support for children and individuals at risk by sharing information with relevant agencies.

Safeguarding of economic well-being of certain individuals

- To protect 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.

Occupational pensions:

- Fulfilling the Council's obligation to provide an occupational pension scheme.
- Determining 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.

PART 3: Additional Conditions Relating to Criminal Convictions etc

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

- Processing of criminal offence data for the purposes of pre-employment checks and declarations by an employee in line with contractual obligations.

7. Law Enforcement Processing

Section 31 of the DPA 2018 defines the law enforcement purposes as 'the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'.

The Council is listed as a competent authority for the purposes of law enforcement.

The Council's processing of criminal offence data within this definition extends to criminal investigations and prosecutions where there is a legal basis to do so, including enforcement of housing standards, food health and safety, fly-tipping, licensing and public protection anti-social behaviour.

Section 35(5) of the DPA 2018 sets out that where processing sensitive data is strictly required for law enforcement purposes, the Council must meet at least one of the conditions in Schedule 8 and this must be captured within an Appropriate Policy Document.

The Council processes sensitive data for the law enforcement purposes when the conditions set out in the following paragraphs of Schedule 8 to the DPA 2018 are met:

Statutory etc purposes

- Where the processing is necessary for reasons of substantial public interest.

Administration of Justice

- Where processing is necessary for the administration of justice.

Protecting individual's vital interests

- Where necessary for life and death cases

Safeguarding of children and of individuals at risk

- Where consent is not appropriate because the individual is under 18 or at risk, but the processing is necessary for reasons of substantial public interest, and is to protect them from harm or to protect their well-being.

Personal data already in the public domain

- Where the data subject has deliberately made the information public.

Legal claims

- processing is necessary for the establishment, exercise or defence of a legal claim

Preventing fraud

- where necessary for the purposes of preventing fraud. If this involves sharing data with organisations that do not fall within the definition of 'competent authority', the processing needs to comply with the UK GDPR, and the Council will identify a lawful basis for sharing the data.

8. Data controller's policies as regards retention and erasure of personal data

We will ensure, where special category or criminal convictions personal data is processed, that:

- there is a record of that processing, and that record will set out, where possible, the envisaged time limits for erasure of the different categories of data
- where we no longer require special category or criminal convictions personal data for the purpose for which it was collected, we will delete it or render it permanently anonymous
- data subjects receive full privacy information about how their data will be handled, and that this will include the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

The Council's Information Asset Register sets out the retention period for main types of records.

9. The Council's compliance with the data protection principles

The Council follows the data protection principles set out in Article 5 of the UK GDPR, and Part 3, Chapter 2 of the DPA 2018 for law enforcement processing, as follows:

Principle 1 - Lawfulness, fairness and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The Council will:

- ensure that personal data is only processed where a lawful basis applies, and where processing is otherwise lawful
- only process personal data fairly, and will ensure that data subjects are not misled about the purposes of any processing
- having regard for the purpose of the processing, ensure that data subjects receive relevant information so that any processing of personal data is transparent

Principle 2 - Purpose limitation
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The Council will:

- only collect personal data for specified, explicit and legitimate purposes, and, having regard for the purpose of the processing, we will inform data subjects what those purposes are in a privacy notice
- not use personal data for purposes that are incompatible with the purposes for which it was collected. If we do use personal data for a new purpose that is compatible, and having regard for the purpose of the processing, we will inform the data subject first.
- when we share special category data, sensitive data or criminal offence data with another controller, processor or jurisdiction, we will ensure that the data transfers are compliant with relevant laws and regulations and use appropriate international treaties, data sharing agreements and contracts.

Principle 3 - Data minimisation
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- The Council will collect personal data that is adequate, relevant and limited to the relevant purposes for which it is processed. We ensure that the information we process is necessary for and proportionate to our purposes.

Principle 4 - Accuracy
Personal data shall be accurate and, where necessary, kept up to date.

- Where the Council becomes aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, every reasonable step will be taken to ensure that data is erased or rectified without delay.

Principle 5 - Storage limitation
Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- The Council will only keep personal data in identifiable form as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so. Once we no longer need personal data it shall be deleted or rendered permanently anonymous.

Principle 6 - Integrity and confidentiality
Personal data shall be processed in a manner 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.

The Council will ensure that there appropriate organisational and technical measures in place to protect personal data:

- The Council will maintain an information security policy and data handling policy.
- Staff and other people who process personal data on our behalf get regular training about how to keep information safe.

- The council limits access to your personal information to those employees, or third parties who have a business or legal need to access it.
- Third parties or contractors that the Council engages with will only process your personal information on our instructions or with our agreement, and where they do so they have agreed to treat the information confidentially and to keep it secure.

Accountability Principle

The Council shall be responsible for, and be able to demonstrate compliance with these principles.

The Council will:

- ensure that records are kept of all personal data processing activities under Article 30 of the UK GDPR and section 61 of the DPA 2018, and that these are provided to the Information Commissioner on request
- carry out a Data Protection Impact Assessment for any high risk personal data processing, and consult the Information Commissioner if appropriate
- ensure that a Data Protection Officer is appointed to provide independent advice and monitoring of the departments' personal data handling, and that this person has access to report to the highest management level of the department
- have in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection law.

10. Contact Information

If you wish to contact our Data Protection Officer, you can do so: either by writing to:

Data Protection Officer
Newark and Sherwood District Council
Castle House
Great North Road
Newark
NG24 1BY

Email: privacy@newark-sherwooddc.gov.uk
Tel: 01636 655216