Doncaster Council

Information Governance

Protecting Special Category Data Policy

v.1.0

DATE – June 2018

Information Governance

Policy cover sheet

Policy Title:	Protecting Special Category Data Policy
Related Policies:	Data Protection Policy; Law Enforcement (Data Protection) Policy; Information Security Policy
Contact:	Information Governance Team Information.governance@doncaster.gov.uk
Freedom of Information:	This Policy and all information within it are suitable for release under the Freedom of Information Act 2000
Equality Impact Assessment:	This Policy has been assessed as having a positive impact on protected groups, as it sets out how the Council will safeguard data relating to protected characteristics.
Version:	1.0
Status:	Published

Version control

Version	Changes
1.0	

Contents

1. Introduction

This Policy explains what special requirements the Council must meet when relying on certain processing conditions as their legal basis for processing special category personal data, and how staff can comply with those requirements while carrying out their work. The policy also satisfies the requirement in the Data Protection Act 2018 (DPA 18) for a data controller to have in place an 'appropriate policy document' in these situations.

2. Scope

The Council's Data Protection Policy sets out what staff must do to ensure the processing of personal data complies with the data protection legislation, and which legal basis might apply to the processing of personal data. This Policy applies only to specific circumstances (i.e. processing conditions) where special category personal data is processed, and these are set out in detail herein.

The Policy applies to ALL members and officers of Doncaster Council and third party organisations working on behalf of the Local Authority.

2.1. Law enforcement purposes

This Policy also applies to special category personal data that relates to criminal offences (including suspect offences) where the Council is **not** acting as a 'competent authority'.

The Council will be a competent authority for the processing of some criminal offence data, but not others. A separate legal framework applies to the processing of data relating to criminal offences by competent authorities. The Council's Law Enforcement (Data Protection) Policy applies to the processing of personal data for a law enforcement purpose where the Council is a competent authority. Staff should familiarise themselves with that Policy and make themselves aware of when these other rules apply.

3. Aims

The aims of this Policy are:

- To ensure that all members and officers of Doncaster Council, processors acting on the Council's behalf and third party organisations are aware of which data protection legislation applies to the processing they are conducting;
- To ensure that all members and officers of Doncaster Council, processors acting on the Council's behalf and third party organisations are aware of the principles and lawful conditions that apply under each law;
- To explain the safeguards Doncaster Council operates to protect the rights and freedoms of data subjects when processing special category personal data; and,
- To identify the responsibilities of members, officers and third party organisations in complying with the law that applies in each instance of processing.

4. Definitions

Competent authority - either a body specified in schedule 7 the Act (Local Authorities are not included here) or 'any other per person if and to the extent that the person has statutory functions for any of the law enforcement purposes.'

Law enforcement purpose – 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. This definition includes the alleged commission of criminal offences by the data subject.

Data Protection Legislation – the General Data Protection Regulation (Regulation (EU) 2016/679), the Law Enforcement Directive (LED), the Data Protection Act 2018 (DPA 18 - as amended) [subject to Royal Assent] and any regulations that apply to any of the specified legislation.

Processing – an operation or set of operations which is performed on personal data, or on sets of personal data, such as:

- collection, recording, organisation, structuring or storage,
- adaptation or alteration,
- retrieval, consultation or use,
- disclosure by transmission, dissemination or otherwise making
- available,
- alignment or combination, or
- restriction, erasure or destruction

Special category personal data - processing of:

- data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- genetic or biometric data, for the purpose of uniquely identifying an individual;
- data concerning health; or,
- data concerning an individual's sex life or sexual orientation.

5. Processing personal data for a law enforcement purpose where the Council is not a competent authority

Processing of personal data (including special category personal data) for a law enforcement purpose where the Council is not a competent authority must meet one of the conditions from part 1, 2 or 3 of schedule 1 of the DPA 18 (see respective Appendices A, B and C).

Such processing must be carried out as if the information were special category data, and therefore must meet all other requirements of this policy (except for section 7 below).

6. Compliance with the data protection principles

Processing of special category personal data must comply with the below Principles of the GDPR:

- processing must be lawful and fair, and meet one of the below conditions;

- purposes of processing be specified, explicit and legitimate;
- data be adequate, relevant and not excessive;
- data be accurate and kept up to date;
- data be kept for no longer than is necessary; and
- data be processed in a secure manner.

More information on each principle is given below:

6.1.1. First principle – fair and lawful processing

Processing must not take place unless the reason for processing is derived from legal powers granted to the Council and it does not infringe the GDPR, DPA 18 or any other law.

Subjects must be told that their data is being collected, who is collecting it and what we will do with it. The Council makes this information available through its privacy notices. A privacy notice must be in place and made available to the subject before any information is obtained from them. If personal information is not obtained from the subject directly a notice must be provided to them at the earliest of the below scenarios:

- at the date of the first communication with them or otherwise;
- if data is to be disclosed to another recipient, before the date of disclosure; or,
- at the latest within one month.

6.1.1.1. Processing conditions

In addition, one of the processing conditions from section 7 (below) must also be satisfied.

6.1.2. Second principle – processing purpose

The purpose of processing special category personal data must be specified prior to collection, made explicit to the subject and legitimate. The data can be processed for a further purpose, but no processing must be carried out on it that is incompatible with the initial processing purpose.

For example, information collected for the purpose of collecting council tax must not be used for the incompatible purpose of sending marketing materials.

6.1.3. Third principle – relevancy

The data collected and processed must be adequate, relevant and not excessive for the purpose it is collected. Only the minimum amount of information necessary for the purpose in question must be processed (e.g. shared, collected or requested).

6.1.4. Fourth principle – accuracy

Data must be accurate and kept up to date. Where compatible with the processing purpose, inaccurate data be erased or rectified as soon as it is found to be incorrect. Occasionally, and where possible, data should be verified with the subject to ensure its accuracy.

6.1.4.1. Sharing data

Inaccurate, incomplete or out of date information must **not** be shared. To that end:

- personal data must be verified before being shared;
- an assessment of the accuracy, completeness and reliability of the data must be included when data is shared; and,
- recipients must be informed if personal data is found to be inaccurate or the sharing unlawful.

6.1.5. Fifth principle – retention

Personal data must be kept for no longer than is necessary for the purpose it was collected. A suitable retention period must therefore be established to guide periodic reviews of the personal data held. These retention periods are defined in the Council's Retention Schedule.

Once this retention period has been exceeded the information must be deleted, unless further retention is justified in accordance with the Archiving condition (see Appendix A).

Information must not be retained beyond the defined organisational retention period without these reasons being specified and recorded.

6.1.6. Sixth principle – data security

Data must be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. The Council's Information Security Policy sets out the security requirements that apply to personal data and special category personal data.

6.2. Subject rights

Subjects have the following rights:

- to be informed of our use of their information;
- of access to their information;
- rectify information about them that is inaccurate;
- to have their information erased (the 'right to be forgotten');
- to restrict how we use their information;
- to move their information to a new data controller;
- to object to how we use their information;
- not to have decisions made about them on the basis of automated decision making;
- to object to direct marketing; and,
- to complain about anything the Council does with their information.

The Council's Individuals Rights Procedure provides more information on these rights – they are generally limited in application, and only apply in specific situations. These rights can be restricted in part or whole; for example, for the prevention and detection of crime.

7. Processing conditions for special category data

Processing of Special category personal data will be lawful only if it meets one of the conditions from Article 9 GDPR below:

a) an individual has given explicit consent to the processing of personal data for one or more specified purposes, except where limited by law;

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Council or a person under employment, social security and social protection law or a collective agreement under law **(also see 7.1 below)**;

c) processing is necessary to protect the vital interests of a person or where the person is physically or legally incapable of giving consent;

d) processing by non-for-profit bodies for legitimate activities with appropriate safeguards;

e) processing relates to personal data which have been made public by a person;

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g) processing is necessary for reasons of substantial public interest under law **(also see 7.5 below)**;

h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of law or pursuant to contract with a health professional and subject to the duty of confidentiality **(also see 7.2 below)**;

i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, subject to the duty of confidentiality **(also see 7.3 below)**; or,

j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes **(also see 7.4 below)**.

7.1. b) employment, social security and social protection

Processing under this point of the GDPR must also meet a condition from part 1 of schedule 1 DPA 18 (see Appendix A below).

7.2. h) health and social care

Processing under this point of the GDPR must also meet a condition from part 1 of schedule 1 DPA 18 (see Appendix A below). In addition, for processing under this point of the GDPR to be lawful the data must be processed by or under the responsibility of a professional subject to an obligation of professional secrecy. Under the DPA 18 this includes circumstances in which processing is carried out:

a) by or under the responsibility of a health professional or a social work professional, or

b) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

7.3. i) public health

Processing under this point of the GDPR must also meet a condition from part 1 of schedule 1 DPA 18 (see Appendix A below).

7.4. j) archiving, research and statistics

Processing under this point of the GDPR must also meet a condition from part 1 of schedule 1 DPA 18 (see Appendix A below).

7.5. g) substantial public interest

Processing under this point of the GDPR must also meet a condition from part 2 of schedule 1 DPA 18 (see Appendix B below).

8. Safeguards – processing special category data

Many of the processing conditions from parts 1, 2 and 3 of the DPA 18 require the data controller to have in place an 'appropriate policy document' in order for the condition to be met. **This Policy constitutes the appropriate policy document for these conditions.**

Paragraphs 33-36 of part 4 of schedule 1 of the DPA 18 define the contents and requirements that apply to this Policy. The document must:

- explain how the Council will ensure compliance with the data protection principles (described in section 5 above) when processing information under one of the conditions from parts 1, 2 or 3 of the DPA 18;
- explain the Council's policies as regards the retention and erasure of personal data processed in reliance on of these conditions, giving an indication of how long such personal data is likely to be retained (see section 6.2.4 above);
- be retained, reviewed and (if appropriate) updated from time to time (see section 9 below); and
- made available to the Information Commissioner on request (and without charge).

The specific conditions to which this Policy applies are set out below.

8.1. Part 1 conditions

Paragraph 1 - Employment, social security and social protection

8.2. Part 2 conditions

All conditions of this part of schedule 1.

8.3. Part 3 conditions

Paragraph 30(c) - Administration of accounts used in commission of indecency offences involving children.

Paragraph 31(b) - Extension of conditions in part 2 of this schedule referring to substantial public interest

It is unlikely that either of these conditions will be relied upon by the Council in the conduct of its business.

9. Review and Retention

9.1. Review

This Policy will be reviewed on an annual basis.

9.2. Retention

Each version of this Policy will be retained for a period of seven years from the date of approval.

Appendix A

The most relevant conditions in part 1 of schedule 1 of the DPA 18 to a local authority are:

a. **Employment, social security and social protection**
b. **Health or social care purposes**
c. **Public health**
d. **Archiving, research or statistical purposes**

Appendix B

The most relevant conditions in part 2 of schedule 1 of the DPA 18 to a local authority are:

a. **Statutory, and government purposes**
b. **Administration of justice and parliamentary purposes**
c. **Equality of opportunity or treatment**
d. **Preventing or detecting unlawful acts**
e. **Preventing fraud**
f. **Elected representatives responding to requests**
g. **Disclosure to elected representatives**

Appendix C

The most relevant conditions in part 3 of schedule 1 of the DPA 18 to a local authority are:

a. **Consent**
b. **Protecting individual's vital interests**
c. **Legal claims**