Leicester City Council

Information Governance & Risk Policies and Guidance

Articles 9 and 10 of the
General Data Protection Regulation 2016 (GDPR)

Schedule 1 to the
Data Protection Act 2018 (DPA2018)

Appropriate policy document for the processing of special categories of personal data and personal data about criminal convictions and offences

Document Version: v1.2

Review Date: 01 September 2020

Owner: Head of Information Governance & Risk

Document History

Revision Date	Version Number	Summary of Changes
20180520	V0.1	Original draft
20180525	V1	Amendments suggested by Head of Information Governance & Risk.
20191017	V1.2	Minor textual amendments. Added: Definition of Special Category data Principle 5-details of compliance Article 5(2)-details of compliance Article 9 – details of compliance Review date

Introduction

This document supplements the Council's Information Governance & Risk Policy and its Information Asset Register (its main record of processing activities under Article 30 of the GDPR) and outlines occasions where special category personal data or personal data about (alleged or actual) criminal convictions and offences is processed under certain conditions permitted by sections 10-11 of the DPA 2018 and set out in Parts 2-3 of Schedule 1 to the Act, as required under Part 4 of that Schedule. It outlines the nature of the processing in each case and then summarises why any such processing fulfils the principles in Article 5 of the GDPR as well as explaining relevant retention and erasure policies.

Special Category Data

Special category data is defined at Article 9 GDPR as personal data revealing:

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; or
Data concerning a natural person's sex life or sexual orientation.

Criminal Conviction Data

Article 10 GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

This Policy Document

Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.

This document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

In addition, it provides some further information about our processing of special category and criminal offence data where a policy document isn't a specific requirement. The information supplements our Privacy Notice and Staff Privacy Notice.

Our processing of special category and criminal offence data for law enforcement purposes is not covered in this document. Processing for law enforcement purposes is carried out by us in our capacity as a competent authority and falls under Part 3 of the DPA 2018.

Lawful Basis for Processing

Leicester City Council is a statutory body with statutory functions as set out in The Local Government Act1972, The Local Government Act and the Localism Act 2011. As part of its statutory and corporate functions, we process special category and criminal conviction data under:

- Article 6(b) of the GDPR (processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract)
- Article 6(c) of the GDPR (processing is necessary for compliance with a legal obligation to which HMRC is subject)
- Article 6(d) of then GDPR (processing is necessary to protect the vital interests of the data subject or of another natural person)
- Article 6(e) of the GDPR (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in HMRC)

Conditions for Processing Special Category and Criminal Offence Data

We process special categories of personal data under the following GDPR Articles:

i. Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the ICO or the data subject in connection with employment, social security or social protection.

Examples of our processing include staff sickness absences and political activity declarations.

ii. Article 9(2)(c) – necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

Examples of our processing include work with vulnerable adults, looked after children etc. who may not have capacity to make decisions, particularly where there are safeguarding concerns, plus using health information about a member of staff in a medical emergency.

iii. Article 9(2)(e) – relates to personal data which are manifestly made public by the data subject.

Examples of our processing include using social media posts for investigatory work such as Trading Standards.

iv. Article 9(2)(f) – necessary for the establishment, exercise of defence of legal claims or whenever courts are acting in their judicial capacity.

Examples of our processing include defending claims at Employment Tribunals, for regulatory investigations, defending judicial reviews or other litigation.

v. Article 9(2)(g) - reasons of substantial public interest.

We process special category data in the performance of our statutory and corporate functions when the following conditions set out in the following paragraphs of Part 2 of Schedule 1 to the DPA 2018 are met:

- paragraph 6 (Statutory etc. and government purposes)
- paragraph 8 (Equality of opportunity or treatment)
- paragraph 9 (Racial and ethnic diversity at senior levels of organisations)
- paragraph 10 (Preventing or detecting unlawful acts)
- paragraph 11 (Protecting the public against dishonesty etc.)
- paragraph 12 (Regulatory requirements relating to unlawful acts and dishonesty etc.)
- paragraph 14 (Preventing fraud)
- paragraph 17 (Counselling)
- paragraph 18 (Safeguarding of children and individuals at risk)
- paragraph 19 (Safeguarding of economic well-being of certain individuals
- paragraph 21 (Occupational pensions)
- paragraph 24 (Disclosure to elected representatives)

vi. Article 9 (2)(h) – necessary for… the provision of health or social care treatment or the management of health or social care systems… .

Examples of our processing include the management of social care users' records and provision of services to care users.

vii. Article 9(2)(i) – necessary for the public interest in the area of public health… .

Examples of our processing include the management of infectious diseases.

viii. Article 9(2)(j) – for archiving purposes in the public interest.

The relevant purpose we rely on is Schedule 1 Part 1 paragraph 4 – archiving.

An example of our processing is the transfers we make to the local archive service as part of our obligations under the Public Records Act 1958.

ix. Article 9(2)(a) – explicit consent

In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

Examples of our processing include staff dietary requirements and health information we receive from our customers who require a reasonable adjustment to access our services.

We process criminal offence data under Article 10 of the GDPR

Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations.

Relevant Service Areas

Appendix C of the Council's Information Governance & Risk Policy lists those areas of the Council that exercise law enforcement functions as the following: City Wardens, Corporate Fraud, Education Welfare Services, Environmental Services, Food Safety, Health & Safety, Licensing, Planning, Private Sector Housing, Trading Standards and the Youth Offending Team. Special category data processed in these areas for law enforcement purposes require this appropriate policy document.

In addition, the Council also is required to hold this appropriate policy document for special category data processed in connection with employment, social security or social protection and in the substantial public interest**.**

Relevant processing conditions from Schedule 1

Paragraph 1 – Employment, social security or social protection
Most special category personal data used for Employment is collected under contract. Employees are aware of the relevant terms and conditions of their employment contract, and an employee privacy Notice is issued to all staff. The data is kept separate from other personal data and is solely used for its limited purpose.

Most special category personal data used for social security or social protection is done so under legal obligation or public task. The data is kept separate from other personal data and is solely used for its limited purpose. Data is used to provide service users with services they are entitled to and some significant decisions can be made about them, including, in some instances, by automated processing. Where any such significant decisions are made, service users are informed if automated decision making has taken place.

Paragraph 8 – Equality of opportunity or treatment
Most special category personal data used for equal opportunities monitoring purposes is collected with the explicit consent of the data subject (in some cases through the provision of options such as 'Prefer not to say' on relevant data collection forms). On the rare occasions where the provision of special

category personal data about racial/ethnic origin, religious beliefs, health (i.e. disability status) or sexual orientation is mandatory and is in the substantial public interest, it is processed under this condition, is kept separate from other personal data, and is solely used for this limited purpose.

However, ethnicity data collected under this condition for attendees at outreach and widening participation events/programmes aimed at prospective employees is not kept separate from other personal data so as to enable the long-term tracking and monitoring of the success of those initiatives.

Paragraph 10 – Preventing or detecting unlawful acts
This condition applies to personal data about criminal convictions and offences used:

i) During due diligence screening of prospective major projects, to ensure that the Council does not unlawfully collect the proceeds of crime (see too Paragraph 14 – Preventing fraud and Paragraph 15 – Suspicion of terrorist financing or money laundering, either or both of which may on occasion become relevant). Any personal data about criminal convictions and offences used for such purposes is gathered from reputable public sources.

ii) During the collection of declarations of relevant unspent criminal convictions/criminal records checks by job applicants where answers to those questions are mandatory (see too Paragraph 11 – Protecting the public against dishonesty etc and Paragraph 12 – Regulatory requirements relating to unlawful acts and dishonesty etc). Any data is used solely for the purposes of safeguarding and protecting the public and employees of the Council, is kept separate from other personal data, and is handled in accordance with strict DBS and security check standards.

By virtue of Paragraph 36 of Schedule 1 to the DPA Act 2018, it is not necessary to demonstrate a substantial public interest in the above processing. (This condition will also apply to specific disclosures to the police and other law enforcement agencies upon request, but an appropriate policy document is not required with regard to such processing.)

This condition also applies to special category personal data (e.g. about religious beliefs or political opinions) and/or personal data about criminal convictions and offences used without explicit consent in connection with the Council's obligations under the Prevent duty.

Although much data processing surrounding Prevent matters is predicated on the consent of the individual, on occasion (especially during initial conversations about concerns) there may be a need to process such data in order to meet the substantial public interest in preventing people from being drawn into radicalisation or terrorism. Any personal data processed under this condition is handled very carefully on a strict need-to-know basis both within and, on occasion, beyond the Council (e.g. disclosures to the Leicestershire Prevent Lead or the police) in accordance with Government guidance.

Paragraph 11 – Protecting the public against dishonesty etc.
This condition applies to special category personal data or personal data about criminal convictions and offences collected. The processing of such data is in the substantial public interest in ensuring the safety of the public.

Any personal data processed under this condition is kept separate from other personal data and is solely used for this limited purpose in accordance with strict protocols that are aligned to normal standards and industry-level guidance.

Paragraph 12 – Regulatory requirements relating to unlawful acts and dishonesty etc.
This condition applies to special category personal data or personal data about regulatory activity that is collected. The processing of such data is in the substantial public interest in ensuring the safety of the public, detecting unlawful acts and malpractice or improper conduct.

Any personal data processed under this condition is kept separate from other personal data and is solely used for this limited purpose in accordance with strict protocols that are aligned to normal standards and industry-level guidance.

Paragraph 14 – Preventing fraud
This condition applies to special category personal data or personal data about criminal convictions and offences collected. The processing of such data is in the substantial public interest in ensuring the safety of the public and the best use of public funds.

Any personal data processed under this condition is kept separate from other personal data and is solely used for this limited purpose in accordance with strict protocols that are aligned to normal standards and industry-level guidance

Paragraph 17 – Counselling etc
Most special category personal data or personal data about criminal convictions and offences used during customer/employee counselling or other customer/employee welfare support services is collected with the explicit consent of the data subject (in some cases through the provision of options such as 'Prefer not to say' on relevant data collection forms). On the rare occasions where the collection or use of special category personal data in a counselling/welfare context is not carried out with explicit consent, it would only be because a substantial public interest has been identified and is being acted upon (e.g. to prevent harm arising to the data subject or others by a disclosure to another part of the Council.) On the rare occasions where the collection or use of personal data about criminal convictions and offences in a counselling/welfare context is not carried out with explicit consent, it would only be because an urgent need had been identified for the data to be disclosed (e.g. to the police, to prevent or detect crime – see Paragraph 10 above).

Paragraph 18 – Safeguarding of children and of individuals at risk
This condition applies to personal data about criminal convictions and offences collected in connection with the delivery of services or employment to young people aged under 18 or vulnerable adults, and solely in relation to mandatory

questions asking attendees to declare any relevant unspent criminal convictions where relevant.

By virtue of Paragraph 36 of Schedule 1 to the Data Protection Act 2018, it is not necessary to demonstrate a substantial public interest in such processing. These data are used solely for safeguarding purposes and to ensure that these events can be run in a safe manner for all attendees.

How and why the data processing under the conditions above meets the principles in Article 5 of the GDPR

Principle 1: Lawfulness, fairness and transparency
In every case above:

- An appropriate lawful basis exists. (See Council privacy Notice)
- The processing is fair to the data subjects because it would always fall within their reasonable expectations.
- A privacy notice is supplied in advance outlining the processing (with the possible exceptions of (i) urgent and specific disclosures in connection with personal data revealed in counselling or other welfare services where a real risk emerges to the wellbeing or safety of the data subject or others, and (ii) due diligence screening, where we are processing only publicly available information and where provision of the privacy notice would require disproportionate effort – although in such cases it is always freely available online).

Principle 2: Purpose limitation
As described under each condition above, any such personal data is only processed for these limited purposes and, where technologically/operationally feasible, either is kept separate from other personal data or access is restricted to prevent any additional use.

Principle 3: Data minimisation
In every case above only the minimum personal data is collected to fulfil the purpose listed.

Principle 4: Accuracy
In every case above any inaccuracies in the personal data are corrected without delay to prevent any unnecessary damage or distress to the data subjects.

Principle 5: Storage limitation
In every case above the data is stored in an identifiable form only while it remains necessary for the relevant purpose.

The Council will ensure, where special category personal data or criminal offences data are 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

- 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
- 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
- The Council retain personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To work out the right retention period for personal data, the Council consider the following matters:

- The amount, nature, and sensitivity of the personal data
- The potential risk of harm from unauthorised use or disclosure of personal data
- The purposes for which we process your personal data and whether we can achieve those purposes through other means, and
- Any legal or regulatory requirements.

Once services are no longer required from the Council by a person, the Council will retain and securely destroy their personal information in accordance with its retention & disposal schedule.

Principle 6: Integrity and confidentiality

In every case the data are stored securely using appropriate technological controls and access is highly restricted to certain 'need to know' staff. The information is not routinely shared beyond the Council unless required by law. Appropriate organisational measures are in place such as policies, procedures, guidance and training.

Article 5(2): Accountability principle

The GDPR states that the data controller must be responsible for, and be able to demonstrate, compliance with these principles. The Senior Information Risk Officer, Head of Information Governance & Risk and Caldicott Guardians (for social care personal data) are responsible for ensuring that the Council is compliant with these principles.

The Council will:

- Ensure that records are kept of all personal data processing activities 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

- Appoint and support a Data Protection Officer 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 legislation

Retention and erasure arrangements

These are covered under the storage limitation principle above.

The Council has a retention and disposal schedule in place (see Council Privacy Notice).

APD review date

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

This policy will be reviewed annually or revised more frequently if necessary.

Additional special category processing

We process special category personal data in other instances where it is not a requirement to keep an appropriate policy document. Our processing of such data respects the rights and interests of the data subjects. We provide clear and transparent information about why we process personal data including our lawful basis for processing in our Privacy Notice and Staff Privacy Notice.

Head of Information Governance & Risk
22nd October 2019 v1.2