Data Protection Policy

MANCHESTER
CITY COUNCIL

www.manchester.gov.uk

Document Control

Title	Manchester City Council – Data Protection Policy
Document Type	Approved Policy
Author	Richard Roscoe
Owner	SIRO/CIARG
Subject	Data Protection
Government Security	Official
Created	April 2014
Approved by	Fiona Ledden (City Solicitor)
Date of Approval	4 September 2024
Review due	September 2026 or earlier where there is a change in applicable law or a Council restructure affecting this Policy.

Revision History

Version	Date	Author	Description of change
4.0	27.03.18	Jacqui Dennis, Interim City Solicitor	Approval
5.0	29.04.19	Fiona Ledden, City Solicitor	Revisions Approved
6.0	20.07.20	Fiona Ledden, City Solicitor	Minor Revisions Approved
7.0	28.07.22	Fiona Ledden, City Solicitor	Minor Revisions approved to cover UK GDPR
7.1	03.09.24	Michael Seal, DPO	Biannual review
8.0	04.09.24	Fiona Ledden, City Solicitor	Approval

1. Introduction

The processing of personal data is essential to many of the services and functions carried out by local authorities. Manchester City Council ('the Council') recognises that compliance with data protection legislation (including the UK General Data Protection Regulation ('UK GDPR'), the Data Protection Act 2018 ('DPA') and related legislation) will ensure that such processing is carried out fairly, lawfully and transparently.

Data protection legislation, and Article 8 of the European Convention on Human Rights recognise that the processing of personal data needs to strike a balance between the need for an organisation utilising personal data to function effectively, efficiently and in the wider public interest, and respect for the rights and freedoms of the individual(s) ('data subject(s)') to whom the personal data relates. This policy sets out how the Council intends to safeguard those rights and freedoms.

2. Scope

This policy applies to the collection, use, sharing and other processing of all personal data held by the Council, in any format including paper, electronic, audio and visual. It applies to all Council staff. "Staff" for the purposes of this policy includes all Council officers, including agency staff.

3. Data protection principles

The Council will comply with the principles relating to the processing of personal data set out in the UK GDPR by putting in place processes to ensure that personal data is:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**')

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;(further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes) ('**purpose limitation**')

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**')

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy**')

- 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; (personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of the data subject) ('**storage limitation**')

- 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 (‘**integrity and confidentiality**’)

The Council shall be responsible for, and be able to demonstrate compliance with, the above principles (‘**accountability**’).

Where the Council processes personal data as a ‘competent authority’ for ‘law enforcement purposes’ (i.e. under statutory law enforcement functions) it shall do so in accordance with the version of the data protection principles set out in the Law Enforcement provisions of the DPA. Those principles are similar (but not identical) to the principles applying to more general processing of personal data detailed above.

‘Law enforcement purposes’ are the purposes of 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 safety.

4. Personal data processed by the Council

The Council processes personal data for many reasons, including in relation to the services it provides and in its role as an employer. In most instances the Council will be the data controller (usually alone, but sometimes jointly) in respect of the personal data it processes (i.e. it will determine the purpose and means of the processing); on occasion it may act as a data processor on behalf of another data controller.

Whether acting as a data controller in its own right, or on another’s behalf as data processor, the Council will maintain a record of its processing activities and make this available to the Office of the Information Commissioner (‘ICO’) upon request. Information concerning the processing of personal data in respect of which the Council is a data controller will be communicated by the Council to data subjects by means of appropriate privacy notices.

5. Conditions

The Council will ensure that its processing of personal data (other than law enforcement processing) fulfils the appropriate general condition(s) for processing outlined in the UK GDPR.

Where a ‘special category’ of personal data is processed (this includes information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purposes of identifying an individual, physical or mental health, sex life or sexual orientation), the Council will ensure that one of the additional conditions set out in relation to special categories of personal data in the UK GDPR is also met, along with any further requirements regarding the processing of sensitive personal data set out in other data protection legislation .

While not formally defined as a ‘special category of personal data’ under the UK GDPR, similar additional conditions and requirements also apply to personal data relating to criminal convictions and offences (including personal data relating to the alleged commission of offences and proceedings relating to the commission or alleged commission of offences). When processing such data the Council will ensure that the relevant additional conditions and requirements are met.

Where the Council processes personal data as a ‘competent authority’ for ‘law enforcement purposes’ it shall do so in accordance with the requirements of the law enforcement provisions of the DPA. In all cases such processing will only be carried out where the

individual concerned has given their consent to the processing of their personal data for law enforcement purposes or where the processing is necessary for the performance of a task carried out for law enforcement purposes by a competent authority. Where such processing involves 'sensitive processing' (this is equivalent to the processing of special category personal data under the UK GDPR) the Council will ensure that the processing is strictly necessary and (unless the individual has consented to the processing) that one of conditions for sensitive processing set out in the DPA is met.

6. Individuals' rights

Data protection legislation provides individuals with various rights. An individual's rights include:

1. The right to be provided with specified information about the Council's processing of their personal data ('**the right to be informed**').

2. The right to access their personal data and certain supplementary information ('**the right of access**').

3. The right to have their personal data rectified, if it is inaccurate or incomplete ('**the right of rectification**').

4. The right to have, in certain circumstances, their personal data deleted or removed ('the right of erasure', sometimes knowns as '**the right to be forgotten'**).

5. The right, in certain circumstances, to restrict the processing of their personal data ('**the right to restrict processing**').

6. The right, in certain circumstances, to move personal data the individual has provided to the Council to another organisation ('**the right of data portability'**).

7. The right, in certain circumstances, to object to the processing of their personal data and, potentially, require the Council to stop processing that data ('**the right to object'**).

8. The right, in relevant circumstances, to not be subject to decision-making based solely on automated processing ('**rights related to automated decision making, including profiling**').

In relation to the first right referred to above ('the right to be informed') in general the Council will:

- where the personal data is collected from an individual, provide them with specified privacy notice information, at the time the personal data is collected.

- where the personal data has not been obtained from an individual, provide them with specified privacy notice information within one month; if the Council uses personal data that it has not collected directly from an individual to communicate with that individual, it will provide the specified privacy notice information, at the latest, when the first communication takes place; if disclosure to another recipient of personal data that has not been collected directly from the individual is envisaged the Council will provide the specified privacy notice information, at the latest, before the data are disclosed.

It is to be noted that there are limited specified circumstances in which the right to be informed will not apply.

Where an individual exercises one of the other rights listed above, the Council will respond without undue delay and in any event within one calendar month, subject to the following two exceptions:

- Where further time is necessary, taking into account the complexity and the number of the request(s) from the data subject, the period for responding will be extended by up to two further calendar months. Where such an extension is required the Council will notify the data subject that this is the case within one calendar month of receiving their request.

- Where the request(s) from a data subject are manifestly unfounded or excessive (in particular because of their repetitive character) the Council will ordinarily refuse the request(s). In exceptional cases the Council may instead exercise its alternative right in such circumstances to charge a reasonable fee that takes into account the administrative cost of complying with the request.

Individuals' Rights – Law Enforcement Processing

The rules relating to individual rights are different where the Council processes personal data as a 'competent authority' for 'law enforcement purposes'.

In those circumstances individuals have the following rights:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure or restriction of processing; and
- the right not to be subject to automated processing.

There are no equivalents to the right to object or the right to data portability. Also, the right of access, the right to rectification and the right to erasure or restriction of processing will not apply to 'relevant personal data' in the course of a criminal investigation or criminal proceedings.'

'Relevant personal data' means personal data contained in a judicial decision or in other documents relating to the investigation or proceedings which are created by or on behalf of a court or other judicial authority.

Where an individual exercises their rights in respect of personal data that the Council is processing for law enforcement purposes the Council will ordinarily respond without undue delay and in any event within one calendar month. There is not an option for the Council to extend this for a further period in the case of complex or numerous requests, although the Council can refuse (or make an administrative charge for) manifestly unfounded or excessive requests.

The Council recognises the fundamental nature of the individual rights provided by data protection legislation. The Council will ensure that all valid requests from individuals to exercise those rights are dealt with as quickly as possible and by no later than the timescales allowed in the legislation.

To minimise delays, and to help ensure that the Council properly understands the request being made, it is preferable for requests from data subjects wishing to exercise their data

subject rights to be made in writing. However, a request does not have to be made in writing; a valid request may be made orally.

Ideally, a written request should be made by means of the appropriate online form available on the Council's public website:

Additionally, all requests from data subjects to exercise their data subject rights must:

- Be accompanied by, where necessary, proof of the identity of the data subject and, where applicable, the written authorisation of the data subject (if the request is being made on their behalf by a legal or lawfully appointed representative or authorised agent).

- Specify clearly and simply how the data subject wishes to exercise their rights – this does not mean that an individual needs to refer specifically to a particular right by name or legislative provision (for example, "I would like a copy of my employee file" is sufficiently clear to indicate that the right of access is being engaged).

- Give adequate information to enable the Council to determine whether the right is engaged and to comply (subject to any exemption(s)) if it is.

- Make it clear where the response should be sent.

- Where relevant specify the preferred format in which any information disclosed to the data subject should be provided in.

Data protection law allows exemptions from complying with data subject rights in specific and limited circumstances. The Council will normally apply the exemptions where they are engaged, unless it is satisfied that it is appropriate or reasonable not to do so.

If a data subject exercising one or more of their data subject rights is dissatisfied with the response received from the Council, they may ask for the matter to be dealt with under the Council's information rights complaints procedure:

A data subject also has the right to complain to the ICO if they believe that there has been an infringement by the Council of data protection legislation in relation to the data subject's personal data. A data subject may also pursue a legal remedy via the courts.

Further information on the rights of data subjects is available from the ICO website.

Additional guidance for staff on how to deal with requests to exercise data subject rights is available via the Council's intranet.

7. Further legal requirements

The Council may be required to disclose personal data to a person or organisation other than the data subject by virtue of a court order, or to comply with other legal requirements, including those relating to the prevention or detection of crime, the apprehension/prosecution of an offender, or the collection of taxation/duties.

The Council may also, in appropriate circumstances, make discretionary disclosures of personal data to a person or organisation other than the data subject where it is permitted to do so by law. When deciding whether to exercise its discretion to disclose personal data in such circumstances the Council will always give proper consideration to the data subject's interests and their right to privacy.

External agencies, companies or individuals undertaking processing of personal data on behalf of the Council ("data processors") must be required to demonstrate, via a written contractual agreement, that personal data belonging to the Council will be handled in compliance with data protection legislation and that appropriate technical and organisational security measures are in place to ensure this. Any contractual agreement between the Council and a data processor will contain all the relevant elements specified in data protection legislation.

Any sharing of Council-controlled personal data with other data controllers must comply with all statutory requirements and corporate policies. Where appropriate the Council will enter into a data sharing agreement before sharing personal data with another data controller, particularly where personal data is to be shared on a large scale and/or regularly. Any data sharing agreements entered into by the Council will be reviewed regularly.

Data matching techniques will only be used for specific lawful purposes and comply with any relevant Codes of Practice.

The Council will follow relevant guidance issued by the Government, the ICO and the Biometrics and Surveillance Camera Commissioner for users of CCTV and similar surveillance equipment monitoring spaces to which the public, residents, service users and staff have access and will also strive to ensure that partner organisations involved in joint or multi-agency initiatives seek to do the same. The Council reserves the right to monitor telephone calls, email and internet access in compliance with relevant legislation. This will be handled in line with guidance issued by the ICO and the Investigatory Powers Commissioners Office.

8. Data security

The Council will process personal data in accordance with its Information and Cybersecurity Policy (and other related Policies and Procedures). In order to ensure the security of personal data, the Council has appropriate physical, technical and organisational measures in place. Council staff are required to comply with the Information Security and Cybersecurity Policy.

9. Training

The Council recognises that data protection training is crucial so that all staff understand their responsibilities relating to data protection and the use of personal data. Failure to comply with data protection legislation could lead to serious consequences, and in some cases may result in significant fines or criminal prosecution.

It is the Council's policy that all staff are required to complete the applicable data protection training courses at least once every two years. The majority of staff will be able to access the relevant data protection training course via the Council's intranet. Line managers will be responsible for ensuring that staff without intranet access complete the appropriate training course via alternative means. The Council will monitor completion rates of data protection courses to ensure that all staff are appropriately trained.

In addition to the corporate training, some post-holders are required to undertake further information governance or data protection training where appropriate for a particular role or within a specific service area.

10. Privacy by design and by default

The Council's approach to compliance with data protection legislation will be underpinned by the principles of privacy by design and privacy by default.

'Privacy by design' means that Council will take into account privacy issues from the very outset of planning for an activity that might involve the processing of personal data. When undertaking a new activity privacy considerations will be embedded throughout.

'Privacy by default' means that the Council will ensure that only personal data that is necessary for a specific purpose is processed. The Council will not collect more personal data than is needed for the purposes concerned, process it more than is necessary or store it longer than is needed.

11. Our commitment to data protection

The Senior Information Risk Owner ('SIRO'), via the Corporate Information Assurance and Risk Group ('CIARG'), will be accountable for ensuring compliance with this policy across the Council. The work of the SIRO will be supported at Directorate level by Directorate Senior Information Risk Officers ('DSIROs').

The Council has also appointed a Data Protection Officer ('DPO'). The DPO's responsibilities include:

- Informing and advising the Council and its staff about their obligations to comply with data protection legislation.
- Monitoring compliance with data protection legislation, including managing internal data protection activities, advising on data protection impact assessments, training staff and conducting internal audits.
- Co-operating with and acting as the first point of contact for the ICO.

The Council will ensure that:

- The DPO reports to the highest management level of the Council in respect of their duties as DPO.
- The DPO operates independently and is not dismissed or penalised for performing their task.

The Council will ensure that individuals handling personal data will be trained to an appropriate level in the use and control of personal data.

The Council will ensure that all staff handling personal data know when and how to report any actual or suspected data breach, and that appropriately trained staff manage any breach correctly, lawfully and in a timely manner. Breaches will be reported to the ICO where such reporting is mandatory or otherwise appropriate and shall be done within the required timescales.

The Council will monitor and review its processing activities to ensure these are compliant with data protection legislation.

The Council will ensure that where there is any new or altered processing of personal data it will take appropriate steps (including where necessary a data protection impact assessment)

to identify and assess the impact on data subjects' privacy as a result of the processing of their personal data. The Council will also ensure that appropriate privacy notices are maintained to inform data subjects of how their data will be used and to provide other mandatory or relevant information.

The Council will review and supplement this policy to ensure it remains consistent with the law, and any compliance advice and codes of practice issued from time to time by the ICO.

12. Disciplinary action and criminal offences

Serious breaches by staff of this policy caused by deliberate, negligent or reckless behaviour could result in disciplinary action including dismissal and may even give rise to criminal offences.

13. Sources of information and guidance

This policy is supported by training, awareness and additional guidance made available to staff on the Council's intranet.

The ICO also provides a free helpdesk that can be used by anyone, and a website containing a large range of resources and guidance on all aspects of information law for use by organisations and the public. See the ICO website.