LANCASHIRE
COMBINED COUNTY AUTHORITY

# Data Protection Policy

## Contents



# Policy Statement

# Scope

This policy forms part of Lancashire Combined County Authority's (LCCA) wider Information Governance Policy Framework, that supports delivery of the Combined Authority functions, in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA).

This policy applies to all LCCA officers, any authorised agents working on behalf of LCCA, (including voluntary, temporary, contract and seconded employees) who capture, create, store, use, share, dispose or otherwise process information on behalf of LCCA, or have access to the Combined Authority's information, information assets or IT equipment.

These persons shall be referred to as 'Users' throughout the rest of this policy.

Lancashire County Combined Authority shall be referred to as 'LCCA', 'the authority' or 'we' throughout the rest of this policy.

All users must understand and adhere to this policy and are responsible for the secure handling of information on behalf of LCCA.

This policy relates to all electronic and paper-based information processed on behalf of the authority.

## Definitions

Article 4(1) UK GDPR defines 'personal data' as being any information relating to an identified or identifiable living individual ('data subject'). This means any individual who can be directly or indirectly identified by reference to an identifier such as a name, an identification number, location data, or an online identifier.

## Purpose

This policy sets out how the authority will ensure compliance with its' obligations under data protection law in the processing of personal data and special category personal data relating to our citizens, customers, suppliers and other individuals for a range of purposes.

Employees of the authority and any authorised agents working on behalf of LCCA may use personal information in carrying out their duties.

In order to undertake our statutory obligations effectively, deliver services and meet customer requirements, the authority needs to collect, use and retain information, much of which is personal, sensitive or confidential.

Such information may be about:

- Customers.
- Employees or their families.
- Members of the public.
- Officers of the authority.
- Business partners.
- Other local authorities or public bodies.

We regard the lawful and correct treatment of personal data by the authority as very important to maintain the confidence of our stakeholders and to operate successfully.

To this end, the authority will ensure compliance, in all its functions, with the Data Protection Act (DPA) 2018, the UK General Data Protection Regulation (UK GDPR) and with other relevant legislation.

## Summary of Data Protection Principles

Article 5 (1) UK GDPR (The Principles) state that personal information shall be:

(a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) Accurate and, where necessary, kept up to date;

(e) 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;

(f) Processed in a manner that ensures appropriate security of the personal data against unauthorised processing, accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5 (2) UK GDPR places a legal obligation on the authority as a data controller, to be responsible for, and to be able to demonstrate compliance with the data protection principles.

The authority is committed to ensuring that all processing of personal data complies with these principles.

## Compliance with the Data Protection Principles and Data Protection Legislation

In order to comply with these principles and demonstrate compliance with all data protection obligations as stipulated in data protection legislation, **the authority will**:

1. Appoint a Senior Information Risk Owner (SIRO) and Data Protection Officer (DPO) who will monitor compliance with UK GDPR and other data protection laws.
2. Raise awareness of data protection across the authority.
3. Report to the Audit and Governance Committee by exception.
4. Maintain an Information Governance Policy Framework and review policies and procedures annually.
5. Where appropriate, ensure that a data protection impact assessment (DPIA) is carried out for all new projects which involve the processing of personal data, in line with Article 35 UK GDPR.
6. Ensure a privacy notice is clearly displayed, explaining why the information is being processed, who it is shared with, how it is being shared, the legal gateways for processing, the applied retention periods and the rights of data subjects with respect to their personal data.
7. Ensure that all employees handling personal information on behalf of the authority receive adequate and regular training in Information Governance.
8. Undertake data quality checks to ensure personal data is accurate and up to date.
9. Demonstrate compliance in an accountable manner through audits, spot checks, accreditations and performance checks.
10. Record all personal data processing activities, internally through the register of processing activities and externally through the Information Sharing Gateway with information sharing agreements.
11. Capture and manage all requests from the general public who wish to exercise any rights set out in UK GDPR (e.g. right of access, right to erasure, right to rectification).
12. Support the pseudonymisation and encryption of personal data.
13. Provide a security network using technical measures including an information security management system (ISMS).
14. Investigate all information security breaches and if reportable, report to the Information Commissioners Office within 72 hours.

## Rights of the Individual

The rights of a data subject are set out in Chapter III of the UK GDPR:

- The right to be informed; via privacy notices.
- The right of access; via subject access requests; the timescale to respond to a SAR is **one calendar month** though this can be extended in certain circumstances. SARs must be free of charge; charges can only be made for further copies or where requests for information are unfounded or excessive.
- The right of rectification; inaccurate or incomplete data must be rectified within one month.
- The right to erasure; individuals have a right to have their personal data erased and to prevent processing unless we have a legal obligation to do so.
- The right to restrict processing; individuals have the right to suppress processing. We can retain just enough information about the individual to ensure that the restriction is respected in future.
- The right to data portability; we need to provide individuals with their personal data in a structured, commonly used, machine readable form when asked.
- The right to object; individuals can object to their personal data being used for profiling, direct marketing or research purposes.
- Rights in relation to automated decision making and profiling; UK GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

The authority will ensure that these rights will be exercised, any such requests from members of the public should be directed to Data Protection@lanacshire-cca.gov.uk where the request will be logged and processed.

## Review and Updates

This policy will be reviewed annually by the DPO and updated as necessary.
**Contact Email**: DPO@lancashire-cca.gov.uk

Version Control

| **Title** | |
|---|---|
| **Version number** | 1.0 |
| **Document author(s) name and role title** | Joanne Winston (DPO) |
| **Document owner name and role title** | Josh Mynott (SIRO) |

| **Date of creation** | January 2025 | **Review cycle** | Annual |
|---|---|---|---|
| **Last review** | | **Next review date** | January 2026 |