



Information Governance Policy Framework

Document Control

Title	Information Governance Policy Framework
Document Type	Policy Framework
Author	Joanne Winston (DPO)
Owner	Josh Mynott (SIRO)
Created	November 2025
Review Date	Annually or as and when required

Revision History

Version	Date	Author	Description of Change
V1.0	November 2025	DPO	First Version

Policy Governance

Version	Approving Body/Officer	Date Approved
V1.0	Monitoring Officer	01.02.2026

What is an Information Governance (IG) Framework?

The IG Framework sets the Authority's strategic approach to managing information as a core asset. It establishes principles, priorities, and accountability for lawful, secure, and transparent handling of information across all formats. Covering access, privacy, security, and assurance, it ensures compliance with data protection and freedom of information legislation. The framework includes the overarching IG strategy, supporting policies, and defined roles to safeguard information integrity, maintain public trust, and enable efficient service delivery.

Service Objectives

The Authority must comply with its statutory obligations under the Data Protection Act 2018, Freedom of Information Act 2000, Environmental Information Regulations 2004 and the UK General Data Protection Regulation (UK GDPR).

The Authority's IG service objectives are to:

1. Provide Access to Information

This involves access to official information (via Freedom of Information (FOI) and Environmental Information Regulations (EIR) requests, data subjects' own data (subject access requests). Also crime and taxation investigation information requests, the publication scheme and the transparency code publishing relevant information to the public. The Authority liaises closely with the Information Commissioner's Office (ICO).

2. Manage Information Privacy

Managing information privacy and sharing across the Authority through information sharing agreements, contracts, Data Protection by Design and by Default controls such as Data Protection Impact Assessments, assessing privacy risks and privacy notices showing people what the Authority does with their information.

3. Manage Information Security

Providing information security alongside the Authority's Digital Service. This involves investigating information security incidents, liaising with the Information Commissioner's Office (ICO), promoting data and cyber security controls (such as secure email), promoting security across the Authority, maintaining a risk register and policies and procedures to improve information security. Digital Services maintain a secure network for the council and conform to ISO/IEC 27001:2013 and maintain PSN (Public Service Network) accreditation and manage an information security management system (ISMS).

4. Manage Information Assurance

Providing assurance that the Authority is compliant with its statutory obligations under UK GDPR and other relevant legislation. This involves regular reviews and system audits, managing performance statistics, spot checks, data quality and minimisation, IG eLearning, delivering people's rights, a register of processing activities (ROPA) and liaison with operational services regarding any processing of personal data.

Approach

Continuous enhancement of the IG Framework is a core strategic priority. Change and improvement will be delivered through an annual Strategic Programme supported by a detailed Action Plan.

Scope

The scope of IG, taken at its widest, includes the management of information in all locations and all media. It includes structured information in databases and unstructured information in paper and electronic files. It includes emails and transient documents, work in progress and telephone notes. It includes blogs, wikis and discussion threads. It includes vital records essential to the continuation of the Authority's business and long-term records that must be preserved through many generations.

The framework encompasses all data owned by the Authority and used in the delivery of its services and statutory responsibilities. This includes any information that is held by the Authority on behalf of another agency.

Data Controllers and Data Processors

The UK GDPR applies to personal data 'controllers' and 'processors'.

Controllers

- Under the UK GDPR, a data controller is "the natural or legal person, public authority, agency or other body which alone or jointly with others, determines the purposes and means of the processing of personal data".

Processors

- A processor is responsible for processing personal data on behalf of a controller.

Under UK GDPR a data controller or a data processor can be held liable for a data protection breach. Processors must only act on the documented instructions of a controller. They do however have direct responsibilities under the UK GDPR and may be subject to fines or other sanctions if they don't comply.

Registration with the Information Commissioner's Office

The Data Protection (Charges and Information) Regulations 2018 (made under sections 137 and 138 of the Data Protection Act 2018 (DPA)) requires every data controller that processes personal information to pay a fee to the ICO, unless they are exempt. Failure to do so will result in a fixed penalty.

Under a three-tier system, payment of a fee is mandatory unless an exemption applies.

Fee Structure

Tier 1 (micro-organisations)	Data Controllers that have maximum turnover of £632,000 per annum or no more than 10 members of staff.	£52
Tier 2 (small or medium organisations)	Maximum turnover of £36 million per annum or no more than 250 members of staff.	£78
Tier 3 (large organisations)	Data Controllers who do not meet the criteria for tier 1 or tier 2, have to pay the tier 3 fee of £3,763. All controllers as eligible to pay a fee in tier 3 unless and until they notify the ICO otherwise.	£3,763

Failure to pay exposes a data controller to the risk of a civil monetary penalty (levied by the ICO) of up to £4000.

Lancashire Combined County Authority is registered as a Tier 1 organisation:

Registration reference

ZB860284

Date registered

08 April 2025

Registration expires

07 April 2026

Payment tier

Tier 1

Data controller

Lancashire Combined County Authority

Address

County Hall, Preston, PR1 8XJ

Data Protection Officer

Mrs Joanne Winston

DPO@lancashire-cca.gov.uk

Freedom of information statement

This data controller states that it is a public authority under the Freedom of Information Act 2000 or a Scottish public authority under the Freedom of Information (Scotland) Act 2002

The Lancashire Combined County Authority (LCCA) is made up of the three upper-tier councils in Lancashire:

- Lancashire County Council
- Blackpool Borough Council
- Blackburn with Darwen Borough Council

These councils form the core membership of the LCCA, which was created to manage devolved powers and funding for areas such as housing, transport, skills, and economic development across Lancashire.

Each of these organisations are registered as Data Controllers as follows:

Name	ICO Registration Number	Comment
Lancashire County Council	Z542705X	Tier 3 data controller. Registration renewal 16 th May.
Blackpool Borough Council	Z5720508	Tier 3 data controller. Registration renewal 19 th November.
Blackburn with Darwen Borough Council	Z6166514	Tier 3 data controller. Registration renewal 21 st February.

Legislation

The following legislation is especially relevant to information governance:

- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Human Rights Act 1998 Article 8
- The INSPIRE Regulations 2009 (spatial data)
- Privacy and Electronic Communications Regulations
- Environmental Information Regulations 2004
- The UK General Data Protection Regulation

Roles and Responsibilities

Senior Information Risk Owner (SIRO)

Josh Mynott is the Authority's SIRO. The SIRO is responsible across the Authority for information governance and has overall responsibility for ensuring that information risk does not impact upon the strategic objectives of the Authority.

Data Protection Officer (DPO)

Jo Winston is the DPO and is responsible across the Authority for data protection. The DPO monitors compliance with UK GDPR and other data protection laws.

Digital Services

Blackburn with Darwen Borough Council provide Digital Services to the Authority and maintain a framework of IT security policies, procedures and controls to ensure that security and information assurance requirements are fulfilled across the Authority.

Policies

The Authority has the following policies in place:

- Data Protection Policy
- Freedom of Information Policy
- Information Security Incident Management Policy

Contact

Email: DPO@lancashire-cca.gov.uk

