LANCASHIRE
COMBINED COUNTY
AUTHORITY

Information Security Incident Management Policy

Version 1.0

Document Control

Title	Information Security Incident Management
Document Type	Policy
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 2026	DPO	First Version

Policy Governance

Version	Approving Body/Officer	Date Approved
1.0	Monitoring Officer	01.02.2026

Contents

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

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

2. Purpose

The authority is committed to the principle of ensuring that all personal data is 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.

The authority takes a proactive approach to managing information security concerns and encourages everyone in the authority to report any incident that they feel has or could compromise information security to Information Governance.

Each report is classed as an 'incident' and is fully investigated with regard to any further action that may be needed. Any incidents which meet the definition of 'personal data breach' as set out at Art. 4 (12) UK GDPR are reported to the ICO.

3. Legal Framework

Data Protection legislation (UK GDPR and DPA 2018) make provision for the processing of personal data in the UK.

Personal Data Breach – Definition

Art. 4 (12) UK GDPR defines a 'personal data breach' as:

''a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed''

Examples include:

1. **Sending Personal Data to the Wrong Recipient**: An employee accidentally emails a file containing sensitive personal information, such as names, addresses, and financial details, to the wrong person. This could lead to unauthorised access to personal data.

2. **Lost or Stolen Devices**: A laptop containing unencrypted personal data is stolen from an employee's car. The data on the laptop contains personal information about clients, which could lead to unauthorised access to information.

3. **Unauthorised Access by a Third Party**: A hacker gains access to a company's database and steals personal information, such as customer names, email addresses, and payment details. This could result in identity theft and financial loss for the affected individuals.

Article 5 ULK GDPR (Key principles for processing personal data)

1. **Lawfulness, Fairness, and Transparency**: Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
2. **Purpose Limitation**: Data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. **Data Minimisation**: Data collected should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy**: Personal data must be accurate and, where necessary, kept up to date. Inaccurate data should be erased or rectified without delay.
5. **Storage Limitation**: Data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.
6. **Integrity and Confidentiality**: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
7. **Accountability**: The data controller is responsible for, and must be able to demonstrate, compliance with these principles

Section 2 of the UK GDPR deals with security of personal data.

Article 32 UK GDPR (Security of Processing)

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including:

a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism* as referred to in Article 42 and which may be used as measures by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

**The council uses PSN (Public Services Network certification) and the NHS DSPT (Data Security and Protection Toolkit) completion as approved certification*.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by domestic law.

Article 33 UK GDPR (Notification of a personal data breach to the commissioner)

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:

a) describe the nature of the personal data incident including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
c) describe the likely consequences of the personal data incident;
d) describe the measures taken or proposed to be taken by the controller to address the personal data incident, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The controller shall document any personal data incidents, comprising the facts relating to the personal data incident, its effects and the remedial action taken. That documentation shall enable the Commissioner to verify compliance with this Article.

Article 34 (Communication of a personal data breach to the data subject)

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

4. Personal Data Incident Reporting and Investigation Process

1. If the incident is still occurring the user should take measures to stop it immediately.

2. Complete the information security incident reporting form as soon as you become aware of an incident.

3. Reports from external sources (suppliers, customers, other organisations) should complete the information security incident reporting form on the authority's website.

4. The incident will be recorded and investigated by the authority's Data Protection Officer.

5. The investigation will include completion of an Information Security Incident Risk Assessment which will be used to determine if it is a 'personal data breach', as defined in Art 4 (12) UK GDPR.

6. Officers have a duty to assist with any investigation and to provide information to the Data Protection Officer upon request, and without delay.

7. Personal data breaches must be reported to the ICO by the Data Protection Officer IG Team within 72 hours of being notified of the incident taking place.

5. Contact

Email: DPO@lancashire-cca.gov.uk