Greater Lincolnshire
Combined County Authority

Policy

Information Handling

Purpose

The purpose of this policy is to provide staff with an understanding of how information in their possession should be protected, and how information should be shared with other parties.

Greater Lincolnshire Combined County Authority generates and holds a wide variety of information that must be protected against unauthorised access, disclosure, modification, or other misuse.

Different types of information require specific security measures, and therefore proper classification of information assets is vital to ensure effective information security and management practices are adhered to across the Authority.

Adherence to this policy will provide everyone with guidance to help ensure that correct information classification and handling methods are applied to their day-to-day activities and managed accordingly.

Document Owner	Monitoring Officer
Document Version	V1.0
Approved By	GLCCA 6 March 2025

This document is the property of the Greater Lincolnshire Combined County Authority.

It may not be reproduced or used for any other purpose than that for which it is supplied, without the prior written permission of the Combined County Authority.

Contents

Scope

This policy applies to:

- All information, regardless of format, processed by us;
- Any individual processing information held by us.
- All aspects of information and data processing.

General Principles

You must respect the confidentiality, integrity and availability of information at all times.

All information required to deliver services and conduct business has inherent value and requires an appropriate degree of protection.

When processing information you must ensure it is subject to proportionate and reasonable controls:

- relative to the sensitivity of the information
- in a manner which reduces the risk of compromise or loss

You must process information in a manner which meets legal and regulatory requirements. This includes information received from, or exchanged with, external partners.

You must not access or attempt to access information unless you have a clear and authorised business need.

You must process personal data in accordance with our data protection policy. This supports our obligations under current data protection legislation.

All staff must be subject to appropriate employment checks prior to handling information. This includes verification of identity.

All staff processing information must undertake annual data protection training and maintain an awareness of their individual responsibilities.

Handling and Storing Information

You must:

- adopt a clear desk and clear screen policy.

- store information securely when not in use, for example under lock and key. This applies particularly to sensitive information.

- ensure information is protected to prevent unauthorised access

- only remove information from official premises when necessary. When doing so you must ensure it remains accounted for and always protected in line with the requirements of this policy.

- collect printed material from printers as soon as possible

- use secure printing when the facility is available. This requires you to be physically present at the printer to receive the prints

- encrypt information that you store on portable ICT devices or media:

    - laptops
    - smartphones
    - removable media

- only store ICT, removable media or hard copy information in an unoccupied vehicle if it is secured out of sight in the locked boot of the vehicle and only if the alternative option is less secure.

- exercise discretion when discussing official business in public or by telephone

- avoid being overlooked when working

Before you distribute sensitive information ensure it is the minimum necessary to achieve your aim. For example, only share personal data with those who have a defined business need to see it.

You must redact documents to remove unnecessary sensitive information.

When redacting information, you must ensure it prevents accidental disclosure of data. You must carry out quality assurance checks before releasing the document to ensure redaction is successful.

Transmitting/sending Information

By post or courier:

- consider using a ‘signed for service’ when sending individual mail items containing particularly sensitive information. Your decision should be informed by the additional cost of such a service versus the additional security benefits it provides, for example an audit trail

- you must use a reputable tracking service for bulk transfer of sensitive information via post to a named individual

- packaging must be robust to prevent damage

You must not transfer data using removable media. If no secure alternative exists you must:

- use a reputable tracked service to a named individual
- encrypt removable media using AES 256 encryption
- communicate passwords separately and do not include them with the removable media. You must use a different communication method when providing the password.

By electronic means:

- electronic transfer of official information must occur in a secure manner
- you must encrypt email traffic when emailing sensitive information
- you must check and confirm the email address of the recipient is the intended one before sending
- password protect attachments which contain personal data or other sensitive information to mitigate the risk of sending an email to an incorrect recipient

Destroying Information

You must destroy hard copy information securely when no longer required. You can achieve this by:

- using a crosscut shredder
- using a confidential waste service such as our "blue bin" service

You must always control access to information until it is securely destroyed.

You must not place hard copy information in open waste bins or waste skips.

You must securely delete digital information from hardware and media when no longer required. You should seek advice from the IT service desk if you are unsure how to do this.

Information Sharing and Disclosure

Before sharing information, particularly sensitive information or personal data, you must:

- be satisfied that the request has come from a legitimate source

- if necessary, have taken steps to validate the authenticity of the request
- ensure you are clear on the purpose for which the information is being requested
- ensure you are clear on what is being requested
- where personal data is requested, ensure you have a legal gateway that allows the council to share it
- be satisfied that the request is reasonable and fair, and it is clear why sharing is necessary in relation to the stated purpose
- take reasonable care to avoid oversharing

You may need to document common rules within an information sharing agreement when:

- personal data is being shared to the same partner organisations for an established, repeatable, and agreed purpose
- the sharing normally consists of the same data sets

When personal data is being provided to a supplier or contracted service you must ensure that the sharing is secure and documented within the relevant contract.

Sharing must occur using corporately authorised solutions.

Information disclosure

When receiving a request to disclose information, you must consider:

- the principles of openness and transparency
- the relevant information legislation

The following requests must be sent to the customer information service:

- requests for disclosure under the Freedom of Information Act or Environmental Information Regulations
- requests by individuals for copies of the personal data we hold about them. This is known as a subject access request under the UK General Data Protection Regulation.
- Information must only be shared with third parties when there is a legitimate and lawful purpose. All instances of information sharing that involves personal data should be documented.

Security Incidents

All security incidents involving information must be reported in accordance with the Security Incident Policy.

Further Information

For further information regarding information handling within the school please contact:

customerinformationservice@lincolnshire.gov.uk

or write to

Customer Relations Team,
Lincolnshire County Council,
County Offices,
Newland,
Lincoln,
LN1 1YL

Further advice and information is available from the Information Commissioner's Office at www.ico.org.uk.

Review

This policy shall be reviewed annually.