Greater Lincolnshire
Combined County Authority

Policy

Security Incident Reporting

Purpose

A security incident is any fact or event that results in the compromise, misuse, or loss of information, ICT assets or ICT services. A security incident can impact the confidentiality, integrity, and, or availability of information.

The purpose of this policy is to:

- Outline the types of security incidents.
- Detail how incidents can and will be dealt with.
- Identify responsibilities for reporting and dealing with incidents.
- Detail procedures in place for reporting and processing of incidents.

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

Contents

Scope

The policy applies to:

- Information which is processed by us or on our behalf by a third party;
- Owned or leased ICT such as PCs; laptops; notebooks; smart phones; software; services, storage media and network resources.

What is a Security Incident?

A security incident is any fact or event that results in the compromise, misuse, or loss of information, ICT assets or ICT services.

A near miss is as any fact or event that has happened, or may have happened, but did not result in a security incident.

A suspected incident is where initial information is sparse, and it may be uncertain whether an actual incident has taken place.

A security incident can impact the confidentiality, integrity, and, or availability of information. Examples of security incidents include:

- the loss or theft of information
- unauthorised disclosure of, or access to, information
- loss or theft of ICT, media, or devices
- physical security breaches
- deliberate or accidental breach of security policy
- insecure disposal of information or ICT assets
- malicious software infection or phishing emails
- social engineering, for example a bogus contractor attempting to use a system

General Principles

We encourage an open and transparent reporting system.

Individuals must report all security incidents accurately and without delay.

Individuals are required to assist in any investigation.

We will record all:

- reported security incidents
- potential security incidents
- near misses
- security weaknesses

We will investigate security incidents in a manner commensurate with the potential impact of the incident.

Where we establish a root cause we will consider corrective action to help prevent similar incidents occurring.

We will determine responsibility for the management of an incident after considering the following points:

- the type of incident
- the type of information involved
- the level of impact or potential impact
- the number and type of stakeholders and partnerships
- the personal data involved
- the source of the incident

Actions on Identifying a Security Incident

As soon as you identify, or suspect, that a security incident has occurred you must take the following action:

- Consider immediate action to contain, rectify or minimise the impact of the security incident e.g. asking an unintended email recipient to permanently delete the email.

- Immediately report all security incidents impacting ICT to cybersecurity@northlincs.gov.uk.

- Immediately report all security incidents to IA@lincolnshire.gov.uk.

- Complete the security incident reporting form which is at [TBC] **Annex A** to this policy and send it to IA@lincolnshire.gov.uk.

Personal Data Breaches

A personal data breach means a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, *personal* data.

Personal data breaches attract several reporting obligations set out in data protection legislation.

All personal data breaches must be recorded.

A personal data breach which is likely to result in a risk to the rights and freedoms of individuals must be reported to the Information Commissioner's Office (ICO) no later than 72 hours from the point we become aware of the breach.

A personal data breach which is likely to result in a *high* risk to the rights and freedoms of individuals must be reported to the impacted individuals without undue delay.

Whether or not a breach meets either of these thresholds will be determined on a case-by-case basis as part of the security incident process. The final decision on reporting requirements is the responsibility of the Data Protection Officer.

Further Information

For further information regarding security incidents please contact:

customerinformationservice@lincolnshire.gov.uk

or write to

Customer Relations Team (GLCCA),
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.

Personal Data Breach Report Form	
Contact Information	
Name of reporter	
Job role	
Contact details	
Incident Summary	
Date and time of incident	
Date and time made aware	
Please describe the incident and, if possible, why it happened.	
Please describe any factors that may have reduced the impact of the incident. e.g. stolen laptop was encrypted; incorrect email recipient has confirmed permanent destruction of email.	
Please indicate the type of information involved (tick all that apply)	**Personal data** ☐ This is any information relating to an identifiable person who can be directly or indirectly identified by it e.g. name, contact details, identification number, email address, location data or online identifier. **Special Categories of personal data** Personal data that relates to the following categories: Race ☐ Ethnic origin ☐ Religious or philosophical beliefs ☐ Trade Union membership ☐

	Sex life ☐ Sexual orientation ☐ Political opinions ☐ Physical or mental health or condition ☐ Genetic data ☐ Biometric data ☐ Criminal convictions or offences ☐ **Other sensitive information** ☐ This is information that does not contain personal data but which could have a negative impact on the school e.g. commercial, legal, or financial data. **Routine information** ☐ Information which is not sensitive and that will not have a negative impact on the school if it was compromised e.g. promotional leaflets.
If personal data is involved, what type of individual does the data relate to?	**Staff** ☐ **Pupil (Child)** ☐ **Parent** ☐ **Governor** ☐ **Other** ☐ (Please explain other here) **Not yet known** ☐
Immediate Action	
What immediate action has been taken in response to the incident? Consider actions to stop the breach and actions to prevent a similar incident happening again.	

Impact on Affected Individual(s)					
What are the potential consequences for affected individuals? For each consequence, please select the likelihood of it occurring.		N/A	Unlikely	Likely	Almost Certain or Confirmed
	Personal Safety	☐	☐	☐	☐
	Safeguarding	☐	☐	☐	☐
	Distress	☐	☐	☐	☐
	Embarrassment	☐	☐	☐	☐
	Interruption to services	☐	☐	☐	☐
	Identity theft	☐	☐	☐	☐
	Fraud	☐	☐	☐	☐
	Financial Loss	☐	☐	☐	☐
	Physical Harm	☐	☐	☐	☐
	Reputational Damage	☐	☐	☐	☐
	Discrimination	☐	☐	☐	☐
	Other (provide details)	☐	☐	☐	☐
	Click or tap here to enter text.				
If personal data is involved, how many individuals could be affected?					
Please describe the potential impact to the person and/or partners and stakeholders. Consider the following areas: • Finance • Reputation • Delivery of education or related service • Legal and regulatory obligations • Other (please provide details)					
Reporting					
Who, internally, has been advised of the incident? Please include names and position.					
Who, externally, has been advised of the incident e.g. Partners, Police.					

If personal data is involved, have the affected individual(s) been notified? If yes please also confirm when they were notified and by whom. If no, please explain why.	
Further Information	
If you have any other information which is useful to the incident report please provide details here.	

Please email the report to IA@lincolnshire.gov.uk