Data Protection Breach Management Policy

Document Control

Organisation	City of Lincoln Council
Title	Data Protection Breach Management Policy
Author – name and title	Becky Scott, Legal & Democratic Services Manager
Owner – name and title	Becky Scott, Legal & Democratic Services Manager
Date	July 2018
Approvals	July 2018- Executive
Filename	Data Protection Breach Management Policy
Version	V.4.1
Protective Marking	Not Protectively Marked
Next Review Date	July 2020

Document Amendment History

Revision	Originator of change	Date of change	Change description
V 1.0	Becky Scott and Matt Smith	April 2014	Published version
V 2.0	Becky Scott	June 2015	Minor amendments
V 3.0	Becky Scott and Matt Smith	May 2016	Amending contacts list and implementing online reporting form.
V4.0	Gavin Thomas	May 2016	Minor changes post proof read
V 4.1	Becky Scott	June 2018	Updating policy in view of General Data Protection Registration (“GDPR”) and new Data Protection Act 2018 (“DPA”), and amendments to roles

Data Protection Breach Management Policy

Background

A data security breach can happen for a number of reasons:

• Loss or theft of data or equipment on which data is stored
• Inappropriate access controls allowing unauthorised use

• Equipment failure
Human error
• Unforeseen circumstances such as a fire or flood
• Hacking attack
• 'Blagging' offences where information is obtained by deceiving the organisation who holds it
• A deiberate act by someone disclosing data

Reason for the policy

The Council has to comply with legal framework for data protection to ensure that all data which is held is protected on behalf of all data-subjects. The Council also has a duty to protect all staff, members and the Council from legal challenge and subsequent cost implications and damage to the Council's reputation.

Time is of the essence

The Council encourages the notification of breaches by staff in accordance with the Data Protection Breach Management Policy at the earliest opportunity. This so that the Council can take immediate steps to recover the data if at all possible, and contain the breach.

Please telephone immediately when the breach/potential breach is noticed the Data Protection Officer or the Legal and Democratic Services Manager or if unavailable a member of the legal team to initially report the breach and provide brief details

Consequences of failing to comply with the DPA

It is recognised that data protection breaches may happen, and that the majority of times it will be human error which has caused the breach. However if individual staff members are found to be have failed to comply with the DPA, it could result in disciplinary action which could lead to dismissal. In addition, an individual can be criminally prosecuted under the DPA and/or liable to pay compensation in any civil action. Timely notification by an individual who thinks a breach has taken place will be taken into account in any resulting disciplinary investigation, as well as assistance in the containment of the breach.

Early reporting of data breaches is essential as under the General Data Protection Regulation which came into force on the 25th May 2018 and the DPA it is mandatory to report certain breaches to the ICO within 72 hours and also to data subjects in certain circumstances. These reports if required will only be made by the Data Protection Officer or Legal and Democratic

Services Manager or if both unavailable a member of the Legal team, after carefully consideration of the risks.

Policy contents

However the breach has occurred, there are four important elements to any breach management plan:

1. Containment and recovery

2. Assessment of ongoing risk

3. Notification of breach

4. Evaluation and response

The policy must be considered to ensure that the Council deals with the breach appropriately and lawfully and there is an online form and a checklist to assist in this process.

Checklist for the Breach Management Policy

1	Contact the Data Protection Officer or Legal and Democratic Services Manager or if unavailable a member of the legal team immediately to report the potential breach	
2.	Contact any other relevant officers (see below) if required plus the relevant Director or Assistant Director and appoint a Lead Officer to investigate the breach.	
3	Complete a Containment and Recovery Plan to maximise the chances of recovering the data, and include procedures for damage limitation – complete the Data Breach Report Form see link below.	
4.	A Risk Assessment will then need to be completed by Data Protection Officer/Legal Services to assess any risks associated with the breach, as these are likely to affect what you do once the breach has been contained. In particular, this is to include potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen	

5	Evaluation and response – it is important the causes of the breach are investigated by Data Protection Officer/Legal Services and that they also evaluate the effectiveness of your response to it and any potential learning points. A report from Audit may be required.	

Contacts

Data Protection Officer	Sally Brooks	Ext 3765	Responsible for data protection matters for the Council and therefore should be notified immediately of any data protection breach
Senior Information Risk Owner	TBC		
Legal Services Manager/ Freedom of Information Officer	Becky Scott	Ext 3441	Freedom of Information Officer
Chief Finance Officer	Jaclyn Gibson	Ext 3258	Responsible for financial matters
BDIT Manager	Matt Smith	Ext 3308	Responsible for all IT security
Audit Manager/Deputy	John Scott/Paul Berry	Ext 3321/3836	Needs to be made aware of any breaches to prepare report
Communications Manager	Steve Welsby	Ext 3318	To be kept up to date on the breach and the actions to be taken
Information Commissioner's Office	0303 123 1113 or 01625 545745		To be informed if a serious breach has occurred, in conjunction with the DPO/Legal Services.

Further information

Legal Services team

To access the Information Commissioner's Office website, click here

To access the Data Breach Report Form, click here

To access the ICO's guidance on Data security breach management, click here