

Information Security Incident Reporting Form

Email completed forms as soon as possible to dpo@nwleicestershire.gov.uk

Provide as much information as you can, but do not delay sending in the form.

For **urgent incidents** (e.g. virus infection), phone the ICT Helpdesk immediately: (01530) 454 718

GENERAL DETAILS	
Incident number:	
Department/Section:	Human Resources
Reporting officer:	
Investigated by:	
Contact number:	
Date form completed:	31 May 2019
Date of incident:	31May 2019
Location of incident	HR computer (desk)
ABOUT THE INCIDENT	
Incident description. What has happened?	Email sent to an extra recipient
How was the incident identified?	Concern re strange message on outlook as attempting to send email
What information does it relate to? e.g. a file containing details of 100 service users name, address, direct debit details.	Short email only which contained an employee's name and information about support we are giving her.
What medium was the information held on? <ul style="list-style-type: none"> - Paper - USB stick - laptop, etc 	Computer – outlook email system
If electronic, was the data encrypted?	No - email
Dealing with the current incident: Please list initial actions: <ul style="list-style-type: none"> - Who has been informed? - What has been done? 	ICT have been informed – they are looking into it as the Service Desk Analyst was not aware of the message I described Email recalled immediately and further email sent to the incorrect recipient apologising and asking them not to read and to delete should the recall have not worked.
Are further actions planned? If so, what?	ICT are unable to advise although they are aware of the box and have said if it happens again to ask them to come up and look at the screen. They have also confirmed the recall was successful.
Have the staff involved in the security incident done any Data Protection Training?	Yes – why I knew it was a data breach
If so, what and when? (Please list)	Learning Pool and various other HR related training

Preventing a recurrence: Has any action been taken to prevent recurrence?	Yes – via ICT	
Are further actions planned? If so, what?		
1.	Was any data lost or compromised in the incident? e.g. loss of an encrypted laptop will not actually have compromised any information, unless e.g. the user was logged in when they lost it.	No
2.	Was personal data lost or compromised? This is data about living individuals such as service users, Councillors or employees. This could be a breach of the Data Protection Act 1998.	Employee name
3.	If yes, was <u>sensitive</u> personal data compromised? This is data relating to health, ethnicity, sexual life, trade union membership, political or religious beliefs, potential or actual criminal offences. This could be a serious breach of the Data Protection Act 1998.	No
4.	Was adult social care, health or public health data involved?	No
5.	What is the number of people whose data was affected by the incident?	1
6.	Is the data breach <u>unlikely</u> to result in a <u>risk</u> to the individual/individuals? Physically, materially, or morally? Example - physical harm, fraud, reputation, financial loss,	Yes
7.	Did people affected by the incident give the information to the Council in confidence? (i.e. with an expectation that it would be kept confidential)	Yes
8.	Is there a risk that the incident could lead to damage to individuals e.g. via identity theft/ fraud? e.g. loss of bank details, NI numbers etc.	No
9.	Could the incident damage an individual's reputation, or cause hurt, distress or humiliation e.g. loss of medical records, disciplinary records etc.?	No
10.	Can the incident have a serious impact on NWLDC's reputation?	No
11.	Has any similar incident happened before in the section?	No
12.	Please confirm you have contacted HR for advice regarding this incident.	Yes
13.	If this incident involves the loss or theft of IT Equipment please confirm you have logged a call on the ICT Help & Support Portal on your desktop?	N/A

FURTHER ACTION: (to be completed by Business Improvement Team)	
Completed by:	
Is further action required?	
Have data subjects been informed?	
Have key stakeholders been informed?	
Have control weaknesses been highlighted and recommendations made?	
Has sufficient and appropriate action been taken?	
Does the incident need reporting to Caldicott Guardian/SIRO?	
Does the incident need reporting to the ICO?	
Does the incident need reporting to IT Security Manager?	
Has the Incident Log been updated?	
Further investigation undertaken by:-	
Date incident closed:-	

1. It is not known who completed the error, so I would recommend the on-line Data Protection training for the whole team.		
2. I do not recommend reporting the incident to the ICO as they are spasmodic incidents. However if trends analysis sees an increase of these errors, then it may have to be a future consideration.		
3. The issue seems to involve operatives not being able to leave their workstations when printing documents, as they need to be ready to take the next call. Printing is left in the back office and documents are put into envelopes when someone is available to carry out the task. I recommend that this process is reviewed, and if possible to have additional printers installed next to desks to minimise the risk of incorrect correspondence being issued and improve efficiencies.		

Evidence from Recommendations	Further Actions	Yes/No

Please contact DPO for any further information:

Nicola Taylor

Data Protection Officer

dataprotectionofficer@nwleicestershire.gov.uk