

Information Security Incident Reporting Form

Email completed forms as soon as possible to dataprotectionofficer@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:	
Reporting officer:	
Investigated by:	Nicola Taylor
Contact number:	
Date form completed:	04.10.19
Date of incident:	03.10.19 – identified 23.08.19 – breach
Location of incident	
ABOUT THE INCIDENT	
Incident description. What has happened?	Emails sent by a former employee to their personal email address on their last day of employment with us. Some of the email attachments relate to internal documents which aren't necessarily an issue, however, some of the attachments are confidential tender documents.
How was the incident identified?	was granted access to the employees emails to enable her to access a sent email that she needed. A number of emails sent on the last day of the employees employment at similar times were identified which seemed suspicious.
What information does it relate to? e.g. a file containing details of 100 service users name, address, direct debit details.	Commercially sensitive information – tender documents, contracts, internal documents. Housing officers names are disclosed although no further personal data has been released.
What medium was the information held on? - Paper - USB stick - laptop, etc	Email
If electronic, was the data encrypted?	n/a
Dealing with the current incident: Please list initial actions: - Who has been informed? - What has been done?	Nicola Taylor – DPO has sent a letter to the ex-employee requesting the emails are deleted. has received confirmation that the emails have been deleted. and NT have assessed what information has been disclosed and feel assured that only minimal personal data has been disclosed (names of officers)
Are further actions planned? If so, what?	No further action
Have the staff involved in the security incident	Yes – although now an ex-employee

done any Data Protection Training?		
If so, what and when? (Please list)	Learning pool	
Preventing a recurrence: Has any action been taken to prevent recurrence?	n/a – isolated incident	
Are further actions planned? If so, what?	No further action	
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.	Yes
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 2018.	Yes
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?	10
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,	No
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)	No
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 DPO)	
Completed by:	Nicola Taylor
Is further action required?	No
Have data subjects been informed?	No
Have key stakeholders been informed?	No
Have control weaknesses been highlighted and recommendations made?	
Has sufficient and appropriate action been taken?	Yes
Does the incident need reporting to Caldicott Guardian/SIRO?	No
Does the incident need reporting to the ICO?	No
Does the incident need reporting to IT Security Manager?	Yes
Has the Incident Log been updated?	Yes

Further investigation undertaken by:-	Nicola Taylor [REDACTED]
Date incident closed:-	10.10.2019

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
Letter to ex-employee to request deletion of emails – confirmation of deletion received.		

Please contact DPO for any further information:

Nicola Taylor

Data Protection Officer

dataprotectionofficer@nwleicestershire.gov.uk