

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:	Complaint 418
Department/Section:	Council Tax
Reporting officer:	[REDACTED]
Investigated by:	[REDACTED]
Contact number:	[REDACTED]
Date form completed:	7 October 2019
Date of incident:	24 June 2019
Location of incident	Atkins Building, Hinckley
ABOUT THE INCIDENT	
Incident description. What has happened?	Forwarding address for [REDACTED] was incorrectly updated to the new forwarding address of her ex husband when the accounts were linked.
How was the incident identified?	Telephone contact from [REDACTED] on 2 September 2019
What information does it relate to? e.g. a file containing details of 100 service users name, address, direct debit details.	Council Tax Demand Notice issued 28 June 2019 and Reminder Notice issued 28 August 2019 were sent to [REDACTED]. The correct address is [REDACTED].
What medium was the information held on? - Paper - USB stick - laptop, etc	Paper
If electronic, was the data encrypted?	Not applicable
Dealing with the current incident: Please list initial actions: - Who has been informed? - What has been done?	[REDACTED] contacted [REDACTED] by telephone to apologise for correspondence being sent to incorrect address, advising that this was due to an administration error when linking her previous jointly & severely liable council tax account with her new sole council tax account. The error had occurred because the first name on J&S was her husband's name and the linked account forwarding address was also amended to his new address.
Are further actions planned? If so, what?	No
Have the staff involved in the security incident done any Data Protection Training?	All Council Tax have been trained in the up to date GDPR regulations.
If so, what and when? (Please list)	GDPR Regulations 24 May 2018, Officer started employment with North West Leicestershire District Council March 2018 and completed this course as part of her induction.
Preventing a recurrence:	Reminder issued to all staff notifying of this breach and must take more care

Has any action been taken to prevent recurrence?	when updating forwarding addresses.	
Are further actions planned? If so, what?	None	
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.	Not as far as we know.
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.	Not unless the letters was opened by ex husband.
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 2018.	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?	One.
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,	Unknown
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?	Unknown
12.	Please confirm you have contacted HR for advice regarding this incident.	No
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?	Not applicable
	12* answered with No, contacted HR as unsure as to why we should notify them, they are going to raise with Legal Department.	

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