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:	Communications
Reporting officer:	[redacted]
Investigated by:	
Contact number:	[redacted]
Date form completed:	27/02/2020
Date of incident:	26/02/2020
Location of incident	Facebook & Twitter
ABOUT THE INCIDENT	
Incident description. What has happened?	A member of the housing team alerted comms to a fraudulent text message a tenant had received about their council tax bill, with a view to us communicating it to the local public. There was an assumption from comms that this had been verified as a fraudulent text. Comms confirmed with Revs & Bens that we don't send text messages to customers about their council tax payments. The offending text message was then Tweeted and Facebooked onto the council's corporate accounts with a warning to local people about the scam.
How was the incident identified?	Revs & Bens called back after realising that there was a possibility that one of the companies that collect money for us could have actually sent a text message out. The housing team member was contacted and couldn't confirm that the text had actually been verified as a scam. At this point the posts on social media were deleted.
What information does it relate to? e.g. a file containing details of 100 service users name, address, direct debit details.	The social media posts contained a reference number – 25127028.
What medium was the information held on? - Paper - USB stick - laptop, etc	It was an image
If electronic, was the data encrypted?	No
Dealing with the current incident: **Please list initial actions:** - Who has been informed?	See the above info. [redacted] has advised no data has been breached. See [redacted] email on what has been done:

- What has been done?	"A little embarrassing but no real harm done. This is not a data breach, there is no personal information just a unique reference number, which will only mean something to the customer, agent and ourselves.. Understand it was only up for 5 minutes or so. Communications Team will not respond in the same way to alleged scams in the future unless it is coming from or substantiated by an agency ...police.. etc due to the risk of the below. [redacted] – will you have a word with [redacted] and also ask her to speak to the customer, let her know it's genuine and she should contact the agent to pay or discuss. [redacted] is there a way the EA can present the message in a way which doesn't generate suspicion from the customer?"
Are further actions planned? If so, what?	
Have the staff involved in the security incident done any Data Protection Training?	Yes with regards to comms staff
If so, what and when? (Please list)	The corporate online training
Preventing a recurrence: Has any action been taken to prevent recurrence?	Yes, we'll be taking extra verification steps should anyone ask us to share a scam message again in the future.
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.	The reference number
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.	No
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?**	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,	
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 – they shared it with us believing it was a scam too.

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.	
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.	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?	No

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