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:	Waste Services
Reporting officer:	[redacted]
Investigated by:	
Contact number:	[redacted]
Date form completed:	23/01/19
Date of incident:	21/01/19
Location of incident	Linden Way Depot via Email
ABOUT THE INCIDENT	
Incident description. What has happened?	An email was sent to [redacted] (member of public) it was intended for [redacted] in our CSC team. I was replying to [redacted] in customer services about an email with photos I received at 13:27pm, which I read on my return after Lunch, at 13:45pm. It include a two photographs of the back of a member of staff and a complaint made by a member of public. Started to reply by entering [redacted] in the "To" bar on reply to email, I received a phone call in the middle of dealing with this which I answered and dealt with, I then came back to the email, typed out my message and didn't fully check it was going to a different [redacted] as this was a member of the public with the same name. I had Emailed him before and his email address was in my address list. I replied to [redacted] straight after he'd reply to me, with my apologies and sorry for any inconvenience caused.
How was the incident identified?	Reply back from member of the public, who was sent the Email in error
What information does it relate to? e.g. a file containing details of 100 service users name, address, direct debit details.	Pictures of a member of staff, presumably urinating. Photograph is of the back of the individual from a distance. Complaint from member of the public in relation to the member of staff urinating. Email address of 6 staff members and 13 members of the public in an Email chain.
What medium was the information held on? - Paper - USB stick - laptop, etc	PC and Email
If electronic, was the data encrypted?	No
Dealing with the current incident: **Please list initial actions:** - Who has been informed? - What has been done?	I received [redacted] reply to make us aware of the error and I emailed him straight back with an apology. [redacted] called me ask about what had happened and not to reply to him. Advised I had already replied with my apology. She asked me not to have any further contact with [redacted] until speaking with management.

Are further actions planned? If so, what?	No
Have the staff involved in the security incident done any Data Protection Training?	Yes
If so, what and when? (Please list)	22.05.18
Preventing a recurrence: Has any action been taken to prevent recurrence?	Double checking addressee on Emails Checking the body of the Email Check CC/BCC boxes Respond to most recent email. Do not reply to chains.
Are further actions planned? If so, what?	To be discussed in weekly team meeting

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.	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 1998.	N/A
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?**	20
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.**	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?**	N/A

FURTHER ACTION: (to be completed by DPO)	
Completed by:	
Is further action required?	No
Have data subjects been informed?	Yes
Have key stakeholders been informed?	No
Have control weaknesses been highlighted and recommendations made?	Yes
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?	No
Has the Incident Log been updated?	Yes
Further investigation undertaken by:-	-
Date incident closed:-	24.01.2019

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**

Please contact DPO for any further information:

Nicola Taylor
Data Protection Officer
dataprotectionofficer@nwleicestershire.gov.uk