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:	Housing Strategy
Reporting officer:	[redacted]
Investigated by:	
Contact number:	[redacted]
Date form completed:	24/06/20
Date of incident:	23/06/20
Location of incident	Email sent to a housing applicant
ABOUT THE INCIDENT	
Incident description. What has happened?	Following the completion of a housing application and the applicant providing their email address, the original email was sent back from a person with the same name and same email address stating that although the email address and name are the same, he has never applied for housing and he doesn't even live here.
How was the incident identified?	Email was picked up this morning by myself whilst checking through Housing Choices emails.
What information does it relate to? e.g. a file containing details of 100 service users name, address, direct debit details.	The email sent is requesting documentation to support the housing application. It contains the service users name, email address and housing application reference number.
What medium was the information held on? - Paper - USB stick - laptop, etc	Housing database
If electronic, was the data encrypted?	no
Dealing with the current incident: **Please list initial actions:** - Who has been informed? - What has been done?	[redacted] read found the email and sent the details to her Manager [redacted] who returned it requesting this form be completed. The officer [redacted] who completed the form has been requested to call the applicant and check the email address etc and advise that the one provided is incorrect.
Are further actions planned? If so, what?	
Have the staff involved in the security incident done any Data Protection Training?	Yes

If so, what and when? (Please list)	
Preventing a recurrence: Has any action been taken to prevent recurrence?	
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 2018.	About another service user.
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,	unlikely
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.	n/k
9.	**Could the incident damage an individual's reputation, or cause hurt, distress or humiliation e.g. loss of medical records, disciplinary records etc.?**	n/k
10.	**Can the incident have a serious impact on NWLDC's reputation?**	n/k
11.	**Has any similar incident happened before in the section?**	n/k
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?**	

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.**	It is not an error by staff, the applicant provided the information	
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