ICT Security Incident Reporting Form

Help Desk Ref: IM029306	Date/Time Call Logged: 20/11/2019 15:22
Date/Time of Incident: 20/11/2019 11:15	Place of Incident: Council Offices
Name & contact details(of person who reported incident): [redacted] Business Focus	
Name(s) of any other persons involved in incident: [redacted], ICT Team	
Equipment involved (including asset numbers, if known) 003215	

Brief description of incident: The user [redacted] received an email yesterday that was quarantined from [redacted]. As [redacted] was expecting an email from the sender she released and opened the email. She then followed the link in the emails and entered her login credentials and followed the prompts, this then caused the email to be forwarded to over 450 different email address.
Has actual loss or harm taken place? (Y/N) : N If Yes give brief details:
Is anyone else aware of the incident? (Y/N): Y If Yes please give details: ICT Team, general user population as we notified them to delete the email
Actions taken to date: Users account disabled, password changed forced, users desktop machine removed and scanned for viruses (with none found) We will be issuing a new desktop to the users and the old one will be wiped.
For use by ICT department

Initial investigation by:	Date/time: 20/11/2011
Brief details of initial actions taken by ICT: Users account disabled, password changed forced, users desktop machine removed and scanned for viruses (with none found) We will be issuing a new desktop to the users and the old one will be wiped. Mail trace run with a list of secondary recipients pass to the users team leader. The users team has contacted all external recipients giving advice and Sam Outama the Head of ICT has sent an all user email out warning users not to open the email and to delete it if received. Copy of breach form passed to Data Protection Officer Nicola Taylor.	
See overleaf for full details of actions taken and planned follow up actions	

Referred to Head of Finance? (Y/N) N	Date: By:

Referred to GCsx? (YN) N	Date: By:
Referred to WARP? (YN) N	Date: By:
Referred to GovCert? (YN)	Date: By:
Details of actions taken:	
Details of planned follow up actions:	