Data Breach Notification Process

(for inclusion in Crisis Management Plans and Incident Management Processes)
In event of a security incident, it is important to understand if there has been a breach of 'personal data' (e.g. names, addresses, email, bank details etc). Under the General Data Protection Regulations (GDPR) A 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

In the event of a Security incident, consider the following;

	Yes/No
Has the incident resulted in the loss of Personal information?	
Was the information unencrypted (i.e. can the information be easily accessed)?	
Is the amount of data lost considered to be a sizeable amount?	
Is the exposure likely to have an impact on individuals rights and freedoms? (i.e. could they suffer financial loss or distress?)	

If the answer to the above to two or more of the above is 'Yes', then the Crisis Management Team must decide on the most appropriate next steps, and either inform the ICO (using the form below) and/or the data subjects.

Please Note: We must notify the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of the personal data breach.

Security breach notification form

This form is for data controllers to report a breach of security to the ICO. It should take about five minutes to complete. Alternatively use the following electronic system to submit the required information - https://report.ico.org.uk/security-breach/

Action Plan
Who is responsible for managing the incident?
Who are the key stakeholders?
How are you going to preserve evidence?
How are you going to maintain an audit trail of actions taken and events?

Key Details
Name of the organisation:
Primary Contact Name:
Job Title:
Email Address:
Contact Number:
Address:
Please provide your Data Registration number (if you have one)

Please provide as much information as possible. This information is required by the ICO to fully understand the nature of the breach. **If not all details are available, then this is an initial notification and full notification must be made within 3 days.**

In addition to completing the form below, we welcome other relevant information, eg incident reports.

Send the completed form to ICO , with **'Security breach notification form'** in the subject field immediately upon completion.

Important information required by the ICO

Please provide as much detail as possible.

1	Have you reported any previous incidents to the ICO? If so, please provide brief details and reference numbers, where known.	
2	When did this incident occur?	
3	Please briefly describe the incident.	
4	Has any personal data been placed at risk? If so, please give us an outline of what this data consists of.	
5	What is the nature and content of the personal data concerned?	
6	Were other providers involved?	
7	Approximately how many data subjects have been affected?	
8	Have you informed the data subjects that this incident has occurred?	
9	Has there been any media coverage of the incident?	
10	Have you taken any action to minimise/mitigate the effect on the data subjects involved? If so, please provide brief details.	
11	Are you carrying out an investigation into the incident - If so when will you complete it and what format will it take?	
12	Have you informed any other regulatory body of the matter? If so, please provide their details and an outline of their response.	
13	What action have you taken to prevent similar incidents in the future?	
14	Is there any other information you feel would be helpful to the ICO's assessment of this incident?	
15	Is this an initial or full notification to the ICO?	