



Appendix A: Data Breach Notification Form

Dale Community Primary School Stonehill Nursery School (delete as appropriate)	
Date	
Reporter name and role	

Part A: Breach Information

When did the breach occur (or become known)?	
Description of Breach. <i>This must include the type of information that was lost, e.g. name, address, medical information, NI numbers</i>	
Which staff member was involved in the breach?	
Has the staff member had Data Protection Training within the last 2 years?	
Who was the breach reported to?	
When was the DPO notified?	
Date Reported:	
Time Reported:	
Initial Actions:	

Part B: Breach Risk Assessment

<p>What type of data is involved?</p>	<p>Hard Copy: Electronic Data:</p>
<p>Is the data categorised as 'sensitive' within one of the following categories:</p>	<p>Racial or ethnic origin: Political opinions: Religious or philosophical beliefs: Trade union membership: Data concerning health or sex life and sexual orientation: Genetic data: Biometric data:</p>
<p>How was the data secured originally?</p>	
<p>How did the breach occur?</p>	
<p>What information was disclosed?</p>	
<p>Whose data has been breached?</p>	
<p>What risks could this pose? Be specific about this situation. If the risk is minimal, explain why.</p>	
<p>Are there wider consequences for the data subjects or school to consider e.g. reputational, loss of confidence?</p>	
<p>How many people might be affected by the breach? Either directly or indirectly.</p>	

Part C – Cyber Breaches

Is this a cyber breach?	Yes/No If 'No' move to Section D
Has the confidentiality, integrity and/or availability of the system been affected. If so which and why	
What is the impact on the organization?	
What is the expected recovery time?	
Are any other IT systems/providers affected? If so, who and how?	

Part D: Breach Notification

Is the breach to be reported to the ICO? With reasons for decision	Yes/No Reasons
Date ICO notified	
Time ICO notified	
Reported by	
Method used to notify ICO	
ICO Reference No.	
Governors' Notified? Yes or No – reasons for decision at this point	
Notes:	
Is the data subject to be notified? Yes / No with reasons	Yes/No Reasons
Date and method data subject notified	
Notified by	
Response	

Part D: Breach Action Plan

Has the data been recovered? Is it likely to be recovered? What steps were taken to recover the data?	Yes/No Reasons
Who has been involved in the data recovery/breach management process?	
Do any other agencies need to be involved? If so, why? (e.g. police and social care)	
What will be done to prevent another breach	
Any training needs identified? For individuals and for whole staff?	