|  |
| --- |
| **Data Breach Report****(to be submitted to the Trust GDPR Manager or the DPO who will advise on further action including the need to report to the ICO).** |
| **SCHOOL \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Name\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_** |
| **Summary of the Breach***Detail the circumstances which have led to the breach including how you become aware of the breach, when the breach occurred and when you became aware of the breach*. |  |
| **Data Type And Individuals Affected** *What information was affected and how many people are affected by the breach. Try and add as much detail as possible including what documents were affected, what information was contained on those documents (for example date of birth, addresses), the categories (for example, parents, staff, children) and number of people affected. You do not need to give names of individuals affected at this stage. However you can also detail any relevant circumstances about individuals which may escalate the breach (for example details of a child protection order, health issues).* |  |
| **Effects Of The Breach** *This could be actual or potential effects (such as loss of confidentiality, breach of security). Detail the risk to the school as well as to the individuals affected and who has received (or could be in receipt of) the data.* |  |
| **Actions Taken***Detail here all actions that have been taken to remedy the breach, including the actions taken by those who accidentally received the information and the actions the school have taken to remedy the breach. Has the breach been contained? If so how was it contained. Has the person who caused the breach been made aware/talked to? Also set dates that these actions have happened where possible. It’s also important to detail here whether the data subject has been notified yet and if not why not (for example because we didn’t foresee there was a high risk).* |  |
| **Data Protection Measures In Place** *Set out here the measures in place (both generally and specific to this situation in question) to protect individual data. For example detail policies in place such as data protection policy, any training that has taken place with staff, security measures to protect emails, password protection, authorised access, etc.). This does not need to be detailed but helps the ICO understand what measures and processes you had in place to prevent this kind of incident from happening in the first place.* |  |
| **Any Other Relevant Information** *To set out here any other relevant information to the breach. For example any future actions you may be taking. Whether there is any further risk to the School of further breaches or affects taking place. If data has been transferred outside of the EU. If there has been previous matters with the ICO in the past. You may also want to summarise here whether you feel the breach has now been contained* |  |
| **Status** *Finally to inform the ICO if any further action is required by the School (i.e. whether further information is required to be provided to the ICO or not or if further investigation is required). For example if you have completed all investigation to say: - We have conducted a review of this incident, details of which have been included in this form If further action is still required to say: - We are conducting a thorough review of this incident and aim to complete such review by [date]. We have included in the attachment to this letter as much relevant information as we have available at this time.* |  |