**DATA BREACH REPORT FORM**

Please complete Sections 1- 8 and send the completed form to: schools.data.protection.officer@enfield.gov.uk

Please ensure your Head and/or Business Manager is aware – however please DO NOT delay reporting if they are not available.

Reporting on this form is on a no-blame basis and the Whistleblowing Policy applies.

It’s more important to get this reported than to get it completely right, so if there are areas that you are unsure of, please say so and submit anyway. In the case of serious breaches we have 72 hours to report to the Information Commissioner, so this should be done without delay.

|  |
| --- |
| **1. Your Details** |
| **Name:** |  |
| **Job Title:** |  |
| **School:** |  |
| **Telephone No:** |  |
| **e-Mail:** |  |
| **Who was the source of the incident?** | [ ]  Internal member/s of staff[ ]  External member/s of staff[ ]  Other third party  |
| **Are you person who is responsible for the incident occurring?** |  [ ]  Yes  [ ]  No*If the answer to this question is ‘no’, then please go to the next section.* |
| **Who was responsible for the incident?** | *Specify the name, team, contact details of the individual/s:* |
| **Date of completion of the form:** | Click or tap to enter a date. | **Time of completion of the form** |  |

|  |
| --- |
| **Details of the incident** |
| **2. Time and date the incident occurred** | **Date:** Click or tap to enter a date.**Time:** |  |
| **3. Time and date the incident was discovered** | **Date:** Click or tap to enter a date.**Time:** |  |
| **4. Did the incident relate to a living person?** | **Yes** [ ] **No** [ ]  |  |
| **6. What is the type of incident** | [ ] Loss of data/device[ ] Theft/stolen of data/device[ ] Disclosure in error (email)[ ] Disclosure in error (verbal)[ ] unlawful destruction of data[ ] accidental/ unauthorised alteration of data [ ] unauthorised access to data |  |
| **What was the format of data that was involved in the incident?** | [ ] Hard copy (paper records)[ ] Digital |  |
| **5. What type of data was involved?** | Please describe the types of data involved in the incident (e.g., Names, NI numbers, addresses, bank details)Tick all types below:[ ]  Non-personal data[ ]  Commercially sensitive data[ ]  Data revealing racial or ethnic origin[ ]  Political opinions[ ]  Religious/ Philosophical beliefs[ ]  Trade union membership[ ]  Sex life data[ ]  Sexual orientation data[ ]  Genetic reassignment data[ ]  Health data[ ]  Basic personal identifiers, eg name, address[ ]  Identification data, eg usernames or passwords[ ]  Economic and financial data eg credit card number, bank details[ ]  Official documents, eg driving licence[ ]  Location data, eg coordinates[ ]  Genetic or biometric data[ ]  Criminal convictions or offences[ ]  OtherIs this data we have received from another organisation?[ ]  Police [ ]  NHS [ ]  DWP [ ]  Other local authorityIf another organisation please specify: |  |
| **What is the format of data that was involved in the incident?** | [ ] Hard copy (paper records)[ ] DigitalPlease forward a copy of the information that was involved in the incident with this form. |  |
| **7. Description of Incident/risk:** |
| **How did you find out that the incident had occurred?** |  |
| **What happened?** |  |
| **Have the internal members of staff received data protection training in the last 2 years to the breach? Please provide dates.** |  |
| **Are there any risks to the data involved in the incident?** | [ ]  *Yes* [ ]  *No* |
| **What are the risks?** |  |
| **8. Mitigation and resolution** |
| **What preventative measures did you have in place to stop this type of breach happening?** | ***Details whether you have any current processes, procedures or technical measures in place.*** |
| **What have you done to mitigate the breach once you were aware?**  | ***Describes steps you have taken to contain the breach and limit its impact*** |
| **What steps have you, or will you take to stop the same or similar breach happening again?** |  |

The following sections will be completed by the Data Protection Team

|  |
| --- |
| **9. If Lost/stolen device** |
| **Name of colleague reviewing** |  |
| **Type of device lost/stolen** | [ ]  Laptop[ ]  Phone[ ]  Tablet[ ]  Other (please specify) |
| **Who is the owner of the device?** |  |
| **Asset no.** |  |
| **Are you aware about where the device may have been lost/ stolen** | *Specify below:* |
| **Is there a risk of unauthorised access to the data on the device** | [ ]  *Yes* [ ]  *No* |
| **What is the risk?** |  |
| **Outcome of Data Protection Review** |  |
| **Date and time** | Date: Click or tap to enter a date.Time: |

Investigating Officer to complete Section 10

|  |
| --- |
| **10. Summary of Investigative Findings – how did this happen** |
|  |
| **Details of Corrective/Preventive Action** |  |
| **Who is responsible for implementing and ongoing monitoring of the actions?** |  |
| **What are the key lessons learnt?** |  |
| **Officer completing investigation name:** |  |
| **Date:** | Click or tap to enter a date. |
| **Suggested date to follow up (according to severity of incident this may be days, weeks or month)** |  |

Data Protection Officer to complete section 11

|  |
| --- |
| 11. **Data Protection Officer Findings (Complete if personal data engaged)** |
| **ICO Report Made?** | [ ]  Yes [ ]  NoICO Case Number:**ICO Case Outcome** |
| **Reason for report / Not reporting** | [ ]  No significant risk to rights and freedoms[ ]  We are not data controller**Decision Details:** |
| **Confirm that the tracker has been updated** | [ ]  Yes |
| **Confirm final investigation report form saved** | [ ]  Yes |
| **Confirm email sent to DSSecurity to close the Service Now ticket** | [ ]  Yes |