**PERSONAL DATA BREACH/INCIDENT REPORTING FORM**

**To be completed by the Investigating Manager**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Author | Policy approved by | Approval date | Review date | Changes made? |
| V1 | IG Team | IG Team | 15.06.2018 | 1.09.2019 | No Changes |
| V2 | IG Team | IG Team | 01.09.2019 | 01.09.2020 | No Changes |
| V3 | IG Team | IG Team | 23.09.2020 | 01.09.2021 | Annual review |
| V4 | IG Team | IG Team | 10.11.2021 | 01.09.2022 | Contacts updated |
| V5 | IG Team | IG Team | 28.10.2022 | 01.09.2024 | Contacts updated |

*Please refer to the Personal Data Breach/Incident Procedure* *while completing this form.*

|  |
| --- |
| **Personal Data Breach/Incident Reporting Form** |
| **School name** |  |
| **Date of incident** |  |
| **Investigating Officer**  | *(School Business Manager/Headteacher)* |
| **Information Asset Owner** | *(Headteacher’s name)* |

***Do not provide the personal details of those involved in the breach or those affected by the breach. Eg. Use ‘service user’ instead of the name of the subject.***

|  |
| --- |
| **What has happened – describe the incident in as much detail as possible with NO acronyms.** Tell us as much as you can about what happened, what went wrong and how it happened. Indicate who was involved without using people’s names eg. service user/manager/pupil etc. |
|  |
| How did you find out about the breach? |
|  |
| When did you discover the breach? |
| Date: Time:  |
| When did the breach happen? |
| Date:Time:  |
| Categories of personal data in the breach  | Y | (Indicate all that apply) | Y |
| Basic personal identifiers eg. Name, contact |  | Identification data eg username |  |
| Finance eg. Credit card, bank details |  | Official docs eg. Driving licence |  |
| Location data |  | Criminal convictions, offenses |  |
| Data revealing racial or ethnic origin |  | Religious or philosophical beliefs |  |
| Political opinion |  | Trade Union Membership |  |
| Sex life data |  | Gender reassignment data |  |
| Health data |  | Genetic or biometric data |  |
| Not known |  | Other – specify  |
| Number of personal data records concerned? |
|  |
| Categories of data subject affected?  | Y | (Indicate all that apply) | Y |
| Pupils |  | Parents |  |
| Governors |  | Employees  |  |
| Not known |  | Other – specify  |
| What are the potential consequences? Please describe the possible impact on the data subject, as a result of the breach. Please state if there has been any actual harm to the data subject(s). |
|  |
| **Risk Analysis Grading – (Please refer to Personal Data Breach/Incident Procedure for further guidance)** |
| Key:**Likelihood**

|  |  |  |
| --- | --- | --- |
| **Number** | **Likelihood** | **Description** |
| 1. | Not occurred | There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trial or forensic evidence. |
| 2. | Not likely or any incident involving vulnerable groups even if no adverse effect occurred. | In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected. |
| 3. | Likely | It is likely that there will be an occurrence of an adverse effect arising from the breach. |
| 4. | Highly likely | There is almost certainty that at some point in the future an adverse effect will happen. |
| 5. | Occurred | There is a reported occurrence of an adverse effect arising from the breach. |

**Impact**

|  |  |  |
| --- | --- | --- |
| Number | Effect | Description |
| 1. | No impact | There is absolute certainty that no adverse effect can arise from the breach – no impact |
| 2. | Minor - Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred | A minor adverse effect must be selected where there is no absolute certainty. |
| 3. | Adverse - Potentially some adverse effect | An adverse effect may be release of confidential information to into the public domain leading to embarrassment or it prevents someone from doing their job. |
| 4. | Serious - Potentially pain and suffering/financial loss | There has been reported suffering and decline in health arising form the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment. |
| 5. | Catastrophic - Death/catastrophic event | A person dies or suffers a catastrophic occurrence |

**Scoring – to be completed by Investigating Officer**

|  |  |  |
| --- | --- | --- |
|  | **Score** | **Comments** |
| Likelihood |  |  |
| Impact |  |  |
| **Total** |  | *Please detail text from risk analysis grid here e.g. reportable to the ICO* |

 |
| Describe the measures you have in place to prevent this type of breach occurring in the first place e.g. staff training, changes to processes/procedures, changes to system controls etc. |
|  |
| Has this type of incident happened before? If so, provide a brief summary of when, who was involved, outcome. |
|  |
| What actions have been taken now to minimise risk of reoccurrence? |
|  |
| Any other actions taken? e.g. where the incident involves the loss of IT equipment have IT been informed? Or if the incident involves social care service user or patient information, have the Council’s Caldicott Guardians been informed? |
|  |
| Have you told the data subjects about the breach?  |
|  |
| **Further action planned – Provide details of all further actions yet to take place** |
|  |

**If you require further advice in relation to this incident please contact:**

**Information Governance Team**

Will Gregory, Information Governance Manager (IG) T. 474 2388; E. will.gregory@stockport.gov.uk

Liz Sykes, Information Governance Manager (IG) T. 474 5157; E. liz.sykes@stockport.gov.uk

Naomi Vhora, CSS Senior Officer (IG) T. 218 1230; E.

naomi.vhora@stockport.gov.uk

**E-mail the completed form to**:

IGschoolsupport@stockport.gov.uk

**Data Protection Officer – Karen Lane E:** **karen.lane@stockport.gov.uk**

**Stage 2 – Completed by the Information Governance Team**

|  |
| --- |
| **Type of Incident, please indicate (Y):** |
| Data posted, faxed, sent by email or verbally disclosed to incorrect recipient |  | Corruption of data (stored or manipulated inappropriately) |  |
| Data deleted or amended in error  |  | Lack of appropriate checks before disclosure eg. redaction/ID checks |  |
| Data deleted or amended maliciously |  | Insecure disposal of hardware |  |
| Loss or theft of paperwork |  | System misuse leading to data disruption |  |
| Loss or theft of unencrypted device |  | Disclosure due to system configuration error |  |
| Loss or theft of encrypted device |  | Inappropriate data being held |  |
| Cyber incident – hacking, disruption |  | Password sharing |  |
| Failure to use BCC when sending email |  | Data processed without consent |  |
| Data stored in an insecure location |  | Data not updated when informed of changes |  |
| Data accessed inappropriately in error |  | Disclosed on Inter/Intranet/ SharePoint |  |
| Data accessed inappropriately deliberately |  | Data obtained by blagging |  |
| Other, give one line indication:  |
| Number of individuals affected [ ] |

|  |
| --- |
| **Investigation chronology:** |
| Date | Description | Further Action |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| **Further questions** |
| Were there measures in place to prevent an incident of this nature occurring? | Y | N | N/K |
| Are there any policies and procedures considered relevant to this incident? |  |  |  |
| Does this incident involve any financial or special personal data? |  |  |  |
| Are the affected individuals aware that the incident has occurred? |  |  |  |
| Have any affected individuals complained to the organisation about the incident? |  |  |  |
| Has the data now been recovered? |  |  |  |
| Had the relevant staff members involved in this incident received training? |  |  |  |
| Have any regulatory bodies been informed about this incident? |  |  |  |
| **Risk analysis review** |
| Assessment | Score | Comments*(Please detail text from risk analysis grid here e.g. reportable to the ICO)* |
| Impact |  |  |
| Likelihood |  |  |
| Total |  |  |
| **Actions** |
| Date | Action | Responsible | Due date | Complete date |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Next Steps |
| Does the risk score require the incident to be referred to the DPO? | Y/NComments: |
| Is there any other reason why this incident should be referred to the DPO? | Y/NComments: |
| IG Officer completing |  |

**Stage 3 – Completed by the Data Protection Officer when Personal Data Breach/Incident form referred**

|  |
| --- |
| **Data Protection Officer Comments:** |
|  |
| Is this incident to be referred to the ICO? | Y/N |  |
| Are there other regulatory bodies that require informing?  |