1. **Data Breach Team**

*Guidance: The first step is to assemble a team to manage and respond to the breach.*

|  |  |
| --- | --- |
| Data Breach Team lead |  |
| Head of Legal | N/A |
| Head of Compliance | N/A |
| Head of IT | N/A |
| [*Insert any other, e.g. Head of HR if the breach involves employee data*] | N/A |

1. **Background information**

*Guidance: Refer to the data breach report form, if appropriate.*

|  |  |
| --- | --- |
| Name of person notifying the actual or suspected breach |  |
| Department and manager |  |
| Date of actual or suspected breach |  |
| Date of discovery of actual or suspected breach |  |
| Date actual or suspected breach notified internally |  |

1. **Preliminary assessment**

*Guidance: As soon as possible, you should take steps to contain the breach and recover lost data. Before you can do this, however, you will need to make a preliminary assessment of what data has been lost, why and how.*

|  |  |
| --- | --- |
| Summary of the facts |  |
| Categories and approximate number of data subjects concerned |  |
| Categories and approximate number of personal data records concerned |  |
| How sensitive is the data? |  |
| Cause of the actual or suspected breach |  |
| Any other comments |  |

1. **Containment and recovery**

*Guidance: Having assembled your data breach team and undertaken a preliminary assessment, containment and recovery should be your first priority. You should consider notifying any relevant insurer, e.g. your cyber, professional indemnity or crime insurer. The insurer/broker can usually provide access to data breach management experts and cyber insurance usually covers breach response costs.*

|  |  |
| --- | --- |
| Does the organisation have cyber insurance? |  |
| Is the actual or suspected breach ongoing? |  |
| What steps can be taken to stop or minimise further loss, destruction or unauthorised disclosure of data? |  |
| What immediate steps can be taken to recover, correct or delete data? |  |
| Should the breach be reported to the police, e.g. is there evidence of theft? |  |
| Does the organisation have crime insurance? |  |
| Does the organisation have any other relevant insurance, e.g. professional indemnity? |  |
| Any other comments |  |

1. **Detailed assessment and record keeping**

*Guidance: Once you have taken steps to contain and recover the data, you should undertake a full assessment and record the breach in a central register.*

|  |  |
| --- | --- |
| What type of data is involved? |  |
| How sensitive is the data? |  |
| Who is affected by the breach? |  |
| What are the likely consequences of the breach on affected data subjects? |  |
| Where data has been lost or stolen, are there any protections in place such as encryption? |  |
| What has happened to the data? |  |
| What could the data tell a third party about the data subject? |  |
| Are there any related or other data breaches? |  |
| Is there a pattern or trend of similar breaches? |  |
| Have you recorded the breach in the organisation's Data breach register? |  |
| Are there wider consequences to consider? |  |
| Any other comments |  |

1. **Notifying data subjects**

*Guidance: In determining whether to notify affected data subjects, you should take into consideration the ICO’s guidance that notification should have a clear purpose, e.g. to warn individuals to take protective action. This is reflected in the table below.*

|  |  |
| --- | --- |
| How can notification help the individual(s)? |  |
| Is there any legal or contractual requirement to notify the data subject? |  |
| Is there a danger of over-notifying?  *Guidance: Not every incident will warrant notification and notifying your entire customer-base of an issue affecting only a small percentage of customers may well cause disproportionate enquiries and work.* |  |
| What is the best way to notify affected individuals? |  |
| Do any individuals or categories of individuals need to be treated with special care? |  |
| What information should be provided to individuals about the steps they can take to protect themselves and what we can do to help them? |  |
| How should affected individuals contact the organisation for further information or to ask questions? |  |
| Will notification help the organisation meet its security obligations? |  |
| Taking the above factors into account, should affected data subjects be notified? |  |
| If yes to the above question:   * Which data subjects should be notified? * How should data subjects be notified? (See Precedents: Letter notifying data subject of data breach – short form and Public statement on data breach. These can be provided if needed.) * What information will be provided? * How will the organisation manage responses or request further information? * How will the organisation track who has been notified? |  |
| Any other comments |  |

1. **Notifying the ICO**

*Guidance: You should notify the ICO when a serious breach has occurred. If you are unsure whether or not to report, the presumption should be in favour of reporting. Consider the factors below and in [section 6.5.2 of the organisation’s data breach plan].*

|  |
| --- |
| **Factor 1: Potential harm to data subjects** |
| [*Insert your conclusions on the potential harm to data subjects*]  *Guidance: This is the overriding consideration in deciding whether a breach of data security should be reported to the ICO. Detriments include emotional distress as well as both physical and financial damage. It can include:*   * *Exposure to identity theft through the release of non-public identifiers, e.g. passport number; or* * *Information about the private aspects of a person’s life becoming known to others, e.g. financial circumstances.*   *Significant actual or potential detriment should be reported, whether because of the volume of data, its sensitivity or a combination of the two.*  *There is no need to report where there is little risk that individuals would suffer significant detriment, e.g. because a stolen laptop is properly encrypted or the information is publicly available.* |
| **Factor 2: Volume of personal data involved in the breach** |
| [*Insert your conclusions on the volume of data involved*]  *Guidance: There should be a presumption to report to the ICO where:*   * *A large volume of personal data is concerned; and* * *There is a real risk of individuals suffering some harm.*   *It will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high, e.g. because of the circumstances of the loss or the extent of information about each individual.* |
| **Factor 3: Sensitivity of data** |
| [*Insert your conclusions on the sensitivity of data involved*]  *Guidance: There should be a presumption to report to the ICO where smaller amounts of personal data are involved that, if released, could cause a significant risk of individuals suffering substantial detriment, including substantial distress.*  *This is most likely to be the case where the breach involves sensitive personal data. If the information is particularly sensitive, even a single record could trigger a report.* |
| **Decision** |
| Taking the above factors into account, we [will/will not] notify the ICO. |

1. **Notifying others**

*Guidance: Consider whether to notify others, e.g. the police, any professional regulator or business partners.*

|  |  |
| --- | --- |
| Is it necessary to notify the police and/or any other relevant law enforcement authority?  *Guidance: You should already have considered this issue for the purpose of containment and recovery (see section 4). Nevertheless, further information may now be available and you should consider this issue again.* |  |
| It is necessary to notify any professional regulator or trade body? |  |
| Is there any legal or contractual requirement to notify any other parties, e.g. pursuant to an outsourcing contract? |  |
| Any other comments | [*Insert comments*] |

1. **Preventing future breaches**

*Guidance: You should evaluate your response to the breach and implement the changes necessary to prevent a recurrence.*

|  |  |
| --- | --- |
| What security measures were in place when the breach occurred? |  |
| What technical and organisational measures could be implemented to prevent the breach happening again? |  |
| Is there adequate staff awareness of security issues? Are there any gaps to fill through training or tailored advice? |  |
| Is it necessary to conduct a privacy risk assessment or to update the organisation’s privacy risk assessment? |  |
| Is it necessary to update the organisation’s privacy risk register? |  |
| Any other comments |  |