**Appendix B – Risk Assessment Matrix**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk** | **Impact** | | | | |
| **Reputational loss** | **Individual** | **Potential detriment** | **Vulnerability** | **Sensitivity** |
| **Low**  **(1)** | The breach is contained within the organisation | The breach has affected 1-9 individual. | The failure does not have the potential to cause detriment to any individual | There is no vulnerability and the individual is at least 18 years old | Personal data has been breached |
| **Medium**  **(5)** | The breach is contained within existing contact with MP’s and local councillors and trusted partners or the breach is no longer in the public domain | The breach has affected between 10 & 99 individuals | The failure has a low risk of resulting in detriment such as anxiety and distress | The individual has a vulnerability that puts them at risk such as a mental health issue, physical disability or is elderly etc. or the breach involves a resident over 18 years old | Sensitive (special Category) data has been breached (e.g. race, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, sexual orientation etc.) |
| **High**  **(20)** | The breach is not contained and there is a chance of social media contact, press coverage etc. | The breach has affected at least 100 individuals | The failure has a high risk of resulting in detriment such as identity theft/fraud/safeguarding concerns | The individual has a vulnerability that puts them at significant risk such as a terminal illness, requires full time care support etc. or where the vulnerability is directly affected by our breach. The incident involves a resident 17 years old or younger | Very sensitive data has been breached such as bank details or detailed health records |

**Assess each of the risks set out above and determine whether to score between low/medium and high**

**Risk Matrix**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk** | **Impact** | | | | | | | | | |  | Totals |
| **Reputational Loss** | **score** | **Individual** | **score** | **Potential Detriment** | **score** | **Vulnerability** | **score** | **Sensitivity** | **score** |  |  |
| **Low** | Low | 1 | 1-9 | 1 | Low | 1 | Low | 1 | Low | 1 |  |  |
| **Medium** | Medium | 5 | 10-99 | 5 | Medium | 5 | Medium | 5 | Medium | 5 |  |  |
| **High** | High | 20 | 100+ | 20 | High | 20 | High | 20 | High | 20 |  |  |
| **Overall risk score** | | | | | | | | | | |  |  |

**Use the above table to score each risk. Instructions are below:**

1. **Please highlight the relevant level for reach risk – low/medium/high Example: For a breach that has occurred within the Council the reputational risk would be highlighted low, whereas personal data that was sent to a resident that has not been contained would be highlighted high. A breach involving 3 individuals would be highlighted 1-9, whereas a breach involving 173 individuals would be highlighted as 100+.**
2. **You should use the numerical values next to each risk to create an overall risk score. For example, if the reputational loss is low, individual is 10-99/medium, potential detriment is low, vulnerability is high, sensitivity is low. This would mean Low = 3, Significant = 5 and High = 20.**
3. **Add the numbers in the Totals column. In the above example, the Overall risk score would be 28.**

**Reporting/Escalation mechanism**

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **Score** | **Data breach owner** | **Reporting/escalation mechanism** |
| Low | <14 | Service Manager | The Data breach investigation remains with the relevant Service Manager. Report to the relevant Service Director, Corporate Data Guardian, Data Protection officer within 24 hours. |
| Medium | Between 15 - 39 | Service Director | The data breach investigation remains with the relevant Service Director. Report to the Corporate Data Guardian, Corporate Director and Data Protection Officer within 24 hours. |
| High | >40 | Corporate Director | Report immediately to Corporate Data Guardian SIRO and Data Protection Officer within 2 hours |

1. **Use the overall risk score to determine whether the data breach is Low, significant or major.**
2. **Use the above reporting/escalation mechanism to determine the data breach owner and who the case should be reported to.**

**Return completed risk assessment matrix along with data protection incident form (Appendix A) to:**

**[data.protection@royalgreenwich.gov.uk](mailto:data.protection@royalgreenwich.gov.uk)**