**GDPR GUIDANCE NOTES – What to do if you have a data breach**

|  |
| --- |
| **What is a data breach?**   * **Confidentiality breach** – seeing personal data one shouldn't. * **Availability breach** – losing control of access to personal data, or inappropriate deletion of personal data. * **Integrity breach** – inappropriate alterations to personal data.   A breach might involve:   * + - * Non-anonymised data being published on the school website showing test results of children eligible for the pupil premium * Safeguarding information about a child being made available to unauthorised people * The theft of a school laptop containing personal data about pupils * Malware software gaining access to emails * Ransomware software resulting in personal data being unavailable or not accessible |

**DO:**

* **What to do if you find or cause a data breach or potential breach**
  + Contact your Head Teacher/Senior Member of staff immediately
  + If you cannot contact the above contact our DPO
  + Gill Smith at gill@mindography.co.uk

**DON’T:**

* **Hope that it will go away**
* Whether you think it is a breach or not notify somebody as soon as possible
* Let the DPO determine whether it is a breach or potential breach and the level of risk and impact on the data subjects
* The DPO and Head Teacher will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  + Lost
  + Stolen
  + Destroyed
  + Altered
  + Disclosed or made available where it should not have been
  + Made available to unauthorised people
* If a data breach has occurred we have 72 hours to investigate it before the ICO needs to be informed.

**What to do if you find or cause a data breach or potential breach**

|  |  |  |
| --- | --- | --- |
| Contact your Head Teacher/Senior Member of staff immediately  If you cannot contact the above contact our DPO Gill Smith  gill@mindography.co.uk |  |  |
| ↓ |  |  |
| Contact DPO who in discussion with the HT will alert the Chair of Governors |  |  |
| ↓ |  |  |
| DPO and School will take all reasonable attempts to contain and minimise the impact of the breach |  |  |
| ↓ |  |  |
| The potential consequences will be assessed – how serious are they and how likely are they to happen? |  |  |
| ↓ |  |  |
| Is it likely that there are risks to someone’s rights and freedoms?  Could the risk put somebody at risk of identity theft, discrimination, damage or threat? |  |  |
| ↓Yes | | No |
| **Report the breach to the ICO within 72 hours**  Go to www.ico.org.uk/for-organisations/report-a-breach/ or call 0303 123 1113.  Provide information on:  • The nature of the breach, including where possible: the categories and approximate number of individuals concerned, the categories and approximate number of data records concerned  • The likely consequences of the breach  • The measures you have taken, or will take, to deal with the breach and mitigate any possible adverse effects on those concerned  Give a point of contact – usually the DPO.  If not all details are available, report as much as possible and explain that there is a delay, the reasons why, and when you’ll have further information. Submit the remaining information ASAP. |  | **Review and record the breach**  Discuss with the Headteacher:   * What happened * How we can stop it from happening again * Whether a process or system regularly has minor incidents   Record:   * Facts and cause * Effects * All decisions taken – including whether or not to report to the ICO/individuals affected * Action taken to contain the breach and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals) |
| ↓ |  |
| Are the r**isk to someone’s rights and freedoms high?**  How serious are the risks? How likely are they to happen? |  |
| ↓Yes |  | No |
| **Inform the affected individual(s) promptly.** Do this in writing and set out your (the DPO’s) name and contact details, the likely consequences of the breach and the measures you have taken, or will take, to deal with the breach and mitigate any possible adverse effects on individuals  **Notify any third parties who can mitigate the impact of the breach eg**  the police, insurers, banks or credit card companies |  |  |