

**Data Breach Notification Procedure**

Where there is a data breach within the College, it is a legal requirement in certain situations to notify the ICO within 72 hours and the individuals concerned as soon as possible. It is essential therefore that all data breaches, no matter how big or small, are reported to us.

This Procedure should be read in conjunction with the Data Protection Policy.

All staff should follow this Procedure. At all stages of this procedure, The Data Protection Officer and management will decide whether to seek legal advice. This procedure will also apply where we are notified by any third parties that process personal data on our behalf that they have had a data breach which affects our data.

The procedure is set out below. Any failure to follow this procedure may result in disciplinary action.

|  |  |
| --- | --- |
| **IDENTIFYING AND REPORTING A DATA BREACH** | |
| If you discover a data breach, however big or small, you must report this via the blank data breach form and send it directly to the Data Protection Officer immediately. The Data Protection Officer can be contacted on 01302 553967, or email [dataprotection@dncolleges.ac.uk](mailto:dataprotection@dncolleges.ac.uk).  Any other questions about the operation of this procedure or any concerns that the procedure has not been followed should be referred in the first instance to the Data Protection Officer.  A data breach could be as simple as you putting a letter in the wrong envelope and therefore even the minor data breaches ***must*** be reported to the Data Protection Officer.  False alarms or breaches that do not cause any harm to individuals or the College should nevertheless be reported as it will evidence learned lessons and best practice to be implemented.  We have a legal obligation to keep a register of all data breaches or potential data breaches. Please ensure that you report any breach, even if you are unsure whether or not it is an actual breach. | |
|  | |
|  |  |

|  |
| --- |
| **BECOMING AWARE OF A DATA BREACH – INVESTIGATING** |
| We become aware of a data breach when we have a reasonable degree of certainty that a security incident has occurred, that has led to personal data being compromised. From this point, our time limit for notification to the ICO will commence.  When you report a data breach to our Data Protection Officer, the Data Protection Officer will promptly investigate the breach to ascertain whether we are fully aware that the breach that has occurred led to personal data being compromised.  **THIS WILL BE DONE WITHIN 24 HOURS OF A BREACH BEING REPORTED TO US.** |

|  |
| --- |
| **ASSESSING /INVESTIGATING A DATA BREACH** |
| Once you have reported a breach and the Data Protection Officer has investigated, if it is decided that a breach has occurred, the Data Protection Officer will log the breach in the Data Breach Register. An initial assessment of the breach will be undertaken, to evaluate its severity.  Once the level of severity is known, the Data Protection Officer will notify management. If necessary, the DPO will appoint a response team which may involve, for example, HR and IT teams and the DPO will assign responsibility for particular tasks as necessary across the response team.  The response team will then investigate the breach and consider any on-going risks to the College and any individuals affected.  If the Data Protection Officer and management consider that the breach is very serious, the appropriate staff will consider the impact on our reputation and the effect it may have on the GDPR assurances we have been entrusted to implement. The Data Protection Officer and senior management will consider whether to appoint a PR professional to advise on reputational damage and will also consider whether legal advice is necessary.  **THIS WILL BE DONE WITHIN 24 HOURS OF US BECOMING AWARE OF THE BREACH.** |

|  |
| --- |
| **FORMULATING A RECOVERY PLAN** |
| The Data Protection Officer and senior management will investigate the breach and consider a recovery plan to minimise risk to individuals. As part of the recovery plan, The Data Protection Officer and senior management may interview key individuals involved in the breach, to determine how the breach occurred and what actions have been taken.  **THIS WILL BE DONE WITHIN 24 HOURS OF ASSESSING THE BREACH.** |

|  |
| --- |
| **NOTIFYING A DATA BREACH TO THE ICO** |
| The ICO has a self-assessment tool to help determine whether your organisation needs to report to the ICO. The outcome of the self-assessment will determine the level of risk to the rights and freedoms of individuals.  If the breach is likely to result in a risk to the rights and freedoms of individuals, the DPO must notify the breach to the ICO within **72 hours** of becoming aware of the breach. We must also notify the individuals concerned as soon as possible where the breach is likely to result in a high risk to their rights and freedoms.  The content of the notification will be drafted by The Data Protection Officer in line with the Data Breach Policy. The notification will be made by the Data Protection Officer. Please be aware that **under no circumstances must you try and deal with a data breach yourself**.  **THIS MUST BE SUBMITTED WITHIN 72 HOURS OF BECOMING AWARE OF THE BREACH.** |

|  |
| --- |
| **NOTIFYING A DATA BREACH TO INDIVIDUALS** |
| We must also notify the individuals concerned as soon as possible where the breach is likely to result in a high risk to their rights and freedoms.  The content of the notification will be drafted by the Data Protection Officer in line with the Data Breach Policy and in conjunction with consulting the ICO if considered necessary. We will notify individuals in clear and plain language and a transparent manner (for example by email, SMS or letter). Please be aware that **under no circumstances must you try and deal with a data breach yourself.**  In some circumstances, explained in our Data Breach Policy, we may not need to notify the identified individuals. The Data Protection Officer will decide whether this is the case.  **THIS WILL BE DONE AS SOON AS POSSIBLE AFTER THE DPO BECOMES AWARE OF THE BREACH.** |

|  |
| --- |
| **NOTIFYING A DATA BREACH TO OTHER RELEVANT THIRD PARTIES** |
| We may also consider that it is necessary to notify other third parties about the data breach depending on the nature of the breach. This could include:   * Insurers * Police * Employees * Parents/Guardians * Sponsors * Banks * Contract counterparties   The decision as to whether any third parties need to be notified will be made by the Data Protection Officer and management. They will decide on the content of such notifications.  **THIS WILL BE DONE WITHIN 5 DAYS OF BECOMING AWARE OF A DATA BREACH.** |

|  |
| --- |
| **CONSIDER WHETHER NOTIFICATIONS NEED TO BE UPDATED** |
| We need to keep the ICO up to date about the data breach. If anything changes from the time we submit the initial notification to the ICO, the Data Protection Officer will consider whether we need to update the ICO about the data breach.  **THIS WILL BE MONITORED AND UPDATED UNTIL RESOLUTION OF THE BREACH IS CONFIRMED BY THE ICO.** |

|  |
| --- |
| **EVALUATION AND RESPONSE** |
| The key to preventing further incidents is to ensure that the College learns from previous incidents.  It is extremely important to identify the actions that the College needs to take to prevent a recurrence of the incident. The Data Protection Officer and management will evaluate as to the effectiveness of our response to the data breach and document this in our Data Breach Register. |