Data Breach Policy

Our policy on reporting significant Breaches of Personal Data is that we will notify our Supervisory Authority [*ICO*] at [*Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF. Tel: 01625 545 745 email: info@ico.org.uk*] within 72 hours or first becoming aware of the Breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Step 1. All staff having been adequately trained and notified, any staff member becoming aware of a data breach shall immediately notify the Data Protection Representative for the company [Jerry Wood mobile: 07720 286694; email: jerrywood@beaumontwood.com] with the following details being recorded (or as much detail as possible to the extent it is known – no delay should be incurred in order to gather data if it is not immediately available):

(a) Description of the incident in as much detail as possible.
(b) Time, date and location of incident
(c) Details of how the incident occurred and any relevant evets leading up to it
(d) If there has been a delay in reporting the incident to the DPR/DPO please explain your reasons for this.
(e) What personal data has been placed at risk? Please specify if any financial or sensitive personal data has been affected and provide details of the extent.
(f) How many individuals have been affected?
(g) Are the affected individuals aware that the incident has occurred?
(h) What are the potential consequences and adverse effects on those individuals?
(i) Have any affected individuals complained to the organisation about the incident?

Step 2. The DPR/DPO, in conjunction with the Board of Directors and Officers shall determine whether the personal data breach is likely to result in a risk to the rights and freedoms of natural persons. If there is uncertainty then it should be assumed that it will.

Step 3. The DPR/DPO, or appropriate alternative, shall notify the Supervisory Authority of the incident within 72 hours.

The following Form can be completed and submitted to the ICO in the event of a Data Breach

https://ico.org.uk/media/for-organisations/documents/2666/security_breach_notification_form.doc

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay, in clear and plain language, the nature of the personal data breach and contain at least the following information and measures:

- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- the likely consequences of the personal data breach;

- the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

This communication to the data subject **shall not** be required if any of the following conditions are met:

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to is no longer likely to materialise;
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.