Reporting a Data Breach to the Data Protection Officer

This procedure applies in the event of a personal data breach, where a breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Examples

A data breach can take many forms, and become evident in different ways, including but not limited to:

- Sending personal data to the wrong person
- Receiving personal data that you should not have access to
- Losing/leaving behind a laptop, phone, USB memory stick, or other device containing personal data
- Losing/leaving behind printed material containing personal data
- Realising that personal data has been altered or deleted inexplicably
- Receiving a query about missing funds from a payment transaction

Procedure – Reporting Personal Data Breaches

If you become aware of a data breach you must contact the Data Protection Officer (DPO) immediately.

This should be done in writing if possible, preferably by email to dpo@kingseducation.com, and should include as much of the following information as possible, but notification must not be delayed waiting for more information:

- The name and contact details of the person making the report
- The nature of the breach (see examples above)
- When the breach became evident
- Who is affected by the breach (e.g. named individuals or groups of people)
- What data has been lost, altered, disclosed, destroyed (if uncertain, name the types of data that may have been affected, e.g. contact, financial, medical details)

The Data Protection Officer will likely contact you for more information so that he or she can make an assessment of whether the breach needs to be reported to the ICO. This assessment can only be made by the DPO and must not be undertaken by any other member of staff. In particular, the fact that some breaches may not be reported to the ICO should not be used as a reason for not reporting a breach to the DPO. Failure to report a data breach may result in disciplinary action.

The Data Protection Officer will also make an assessment of the risk to the data subject. If the Data Protection Officer concludes that the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject, for example, where there is a risk of identity theft, he or she will notify the data subject directly.