Procedure: Data Breach Notification

Procedure Ref: OP/7CA/SP112

Approved By: Principal

Date: October 2020

Signature:

1. Purpose

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

2. Scope

This Procedure should be read in conjunction with our Data Breach Policy and Data Protection Policy. Our Data Breach Policy contains detailed information on what constitutes a data breach; please read it to make sure that you aware of the breadth of the concept of a data breach.

3. Responsibility

This Procedure should be followed by all staff. At all stages of this procedure, our 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 personal data.

4. Procedure

The procedure is set out on the next page. 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 to our Data Protection Officer immediately. The Data Protection Officer is Karen Wilson, and can be contacted at: 01946 839300 ext 1010, karenw@lcwc.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 most minor data breaches ***must*** be reported.

False alarms or even breaches that do not cause any harm to individuals or to the College should nevertheless be reported as it will enable us to learn lessons in how we respond and the remedial action we put in place.

We have a legal obligation to keep a register of all data breaches, no matter how big or small and no matter whether any harm was caused. Please ensure that you do report any breach, even if you are unsure whether or not it is a 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, our Data Protection Officer will promptly investigate the breach to ascertain whether we are fully aware that are breach has occurred that has led to personal data being compromised.

THIS WILL BE DONE WITHIN 24 HOURS OF A BREACH BEING REPORTED TO US.

ASSESSING A DATA BREACH

Once you have reported a breach and our Data Protection Officer has investigated it and has decided that we are aware that a breach has occurred, our Data Protection Officer will log the breach in our Data Breach Register and will carry out an initial assessment of the breach to evaluate its severity.

Once the level of severity is known, our Data Protection Officer will notify management. If necessary, we will appoint a response team which may involve for example our HR and IT teams and we will assign responsibility for particular tasks as necessary across the response team.

We will then investigate the breach and consider any on-going risks to the College and any individuals affected.

If our Data Protection Officer and management consider that the breach is very serious, they will consider the impact on our reputation and the effect it may have on the trust placed in us. Our 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 needed.

THIS WILL BE DONE WITHIN 24 HOURS OF US BECOMING AWARE OF THE BREACH.