

ICO Imposes £120,000 Fine For Sensitive Personal Data Breach

Many people will be familiar with the mistake of sending an e-mail to the wrong recipient, but Surrey County Council recently was faced with the financial consequences of making the mistake of e-mailing sensitive personal data.

The UK Information Commissioner's Office (ICO) on June 9, 2011, served Surrey County Council with a hefty £120,000 (approximately U.S.\$194,000) monetary penalty for e-mailing personal information to the wrong recipient on not one, but three separate occasions.

The first breach under the Data Protection Act occurred back in May 2010, when a file containing 241 different individuals' data was leaked via a group e-mail from a member of staff working within the Adult Social Care Team. The data contained in the file related to the physical and mental health of the 241 individuals; physical and mental health of course being some of the most sensitive information there is about a person. This data was e-mailed to the Council's transport contacts, including taxi firms and bus hire companies. Critically, the data was not password protected nor encrypted.

The ICO considered this first breach by the Council to be the most severe.

The following month after the initial breach, the Council sent more personal information to a group of recipients who had signed up for the Council newsletter.

Following the second data breach, a member of the Council's Children Services department sent an e-mail on January 21, 2011, containing information relating to the health of a particular individual to the wrong internal e-mail group. This third data leak involved only the internal network of the Council and is therefore perhaps considered to be less serious than the first two; however, the breach was still considered by the ICO to be a breach of the data protection legislation.

Council Adopts New Security Measures

As a result of these breaches of the Data Protection Act, the Council have adopted new measures to implement their privacy policies so to prevent sensitive information landing in the hands of the wrong recipient. An example of the new measures is the introduction of a warning system alerting staff before they e-mail sensitive data to an external source.

Having sufficient security measures in place is crucial for businesses and organisations handling data of a sensitive and personal nature. To do otherwise is in breach of the Act and risks severe consequences!

The [ICO's news release](#) about the Surrey County Council breach is available on its website.

Valerie Surgenor is a Partner in the IP, Technology & Commercial group at MacRoberts LLP. For further information, please contact valerie.surgenor@macroberts.com.

This article appeared in the June 2011 edition of the World Data Protection Report.

[See our website for full Copyright notice and Disclaimer.](#)

© MacRoberts LLP 2011