Beyond the ICO fine: the true impact of a data breach on your alumni

By John Rux-Burton, Founder and Managing Partner, Rux Burton Associates

We wait with bated breath for the government to be fined £2.8b (4% of turnover) for publishing the addresses of the New Years' honour recipients online. Of course, it won't happen and it would only move our money from one government coffer to another.

But what about when your school experiences a data breach? There were some 300 public figures on the New Years' honours list, many of whom were security-sensitive individuals on the cabinet office list. There are quite a few institutions who could assemble just as sensitive a list indeed some much more so; there are alumni who are deliberately not in the public eye but might well be of interest to bad people. When your data is exposed it's not just whether the ICO will forgive you. Will your alumni?

However, you need your alumni, more than the cabinet office needs these public figures. Upsetting musicians and cricketers is annoying to politicians but disastrous indeed if you are planning a concert or sports hall appeal. And, let's face it, the real loss is one of trust. No one trusts government but they do trust you. Lose their data and they won't; whether they are a famous actor or a bank clerk from Tooting, a data breach, even if inadvertent, will impact on your relationship with your alumni.

So, how do we avoid data breaches? Firstly, keep your data under lock and key and let it out only when you have to. That means not adding in any unnecessary exchanges. For example, if you have given a consultant the data to run a phone campaign, why are you then sending the data off to a separate mailing house to print? Limiting the opportunity for a breach is common sense and easily fixed.

More complex to resolve is the tendency to try and find work arounds to GDPR. For example, solving (PCI) by taking single direct debits is no solution at all. Instead of fixing security one has simply sidestepped the regulations. There is nothing wrong with single direct debits, but taken in an insecure way they can still lead to fraud. And if your system has fundamental security question marks (which if your software cannot achieve PCI compliance it does) then what about the security of the rest of your data? If the cabinet office had lost the credit card details of all the new year honours' list, then their PAs would simply have ordered new ones and the breach would be over. No one would be considering moving house. It's amazing how institutions will worry their network is insecure and so get landlines so they can 'safely' talk to their alumni, but then put immensely sensitive information gleaned in that call onto a piece of software that cannot offer payment card industry security standards.

With the ICO's new draft code of direct marketing currently under consultation, it is as good a time as ever to review your data protection policies and procedures to avoid data

breaches such as the government's. Your school should make sure they laud their achievers without taking risks with their data through needless transfers and unattested software. It's because they trust us, they give us all their personal information. Let's keep that trust.