

Education sector accounts for 15% of data breaches

The Information Commissioner's Office (ICO) has recently published the latest statistics on reported data breaches. Between November 2019 and January 2020 a total of 2,795 data breaches were reported, with just over 15% of the occurrences originating in the education sector.

10 March 2020

The Information Commissioner's Office (ICO) has recently published the latest statistics on reported data breaches. Between November 2019 and January 2020 a total of 2,795 data breaches were reported, with just over 15% of the occurrences originating in the education sector.

In this article Dai Durbridge reviews the data and highlights some lessons learned that could be implemented in your school to help you reduce risk and avoid unnecessary financial penalties.

Over the three-month period, 429 data breaches were reported across the education sector. Of the 24 different business areas recorded, only the health sector reported more – with 542 individual cases reported.

We should not, however, read too much into these numbers, as they could tell us very different things: on the one hand yes, there are still a lot of breaches in the sector; but on the other hand, education institutions could just be much better than others at reporting them. Or what is more likely, it could be something in between. What is of interest – and extremely useful – are the types of breach reported.

Data breaches are divided into 20 different breach categories, covering everything from malicious cyber threats to the incorrect disposal of data. The list below includes the top five types of breaches reported in the education sector, along with a couple of other interesting ones:

Type of breach	Number of breaches
Data emailed to wrong recipient	48
Loss of paperwork	41
Phishing attacks	39
Posted/faxed to wrong address	26
Loss of devices	24
Unauthorised access to data	20
Failure to redact information	15

You probably recognise these are risk areas in your school. The two interesting ones are, well, interesting: 15 reported breaches for schools failing to redact information, and a further 20 breaches caused by unauthorised access to data.

Over the last couple of years we have advised many clients following data breaches. If you asked me to guess the top three behaviours likely to cause a data breach in schools, I would say:

1. Emails sent to the wrong recipient;
2. Loss of paperwork; and
3. Unauthorised data access.

The wider sector statistics reported by the ICO are certainly in line with what we are seeing from our clients.

Now you know what the key risks are, you should consider the extent to which they are risks in your school or trust and what steps you may need to take to minimise them. You should consider the following:

Emails

- If you still have the autocomplete function turned on for email addresses you should disable it. The autocomplete function can lead to emails being sent to the wrong person because the sender tends to assume the autocomplete has chosen the correct recipient.
- Make sure you are using password protected documents and not putting personal data in the main body of emails.

Loss of paperwork

- Reflect on whether your staff needs to take paperwork off the school site or whether there is a better way for them to access the data they need.

Unauthorised access

- In many cases, unauthorised access to data can be avoided by individuals being vigilant. Staff should be reminded to lock their computers when they leave their desks and take notice of those around them (especially the more mischievous pupils) when personal data is being viewed on screen. It is very easy for photos to be taken and shared.

Given that the top three types of data breach account for over a quarter of all education breaches, you can improve your GDPR compliance by simply focussing on these issues.

Contact



Dai Durbridge

Partner

dai.durbridge@brownejacobson.com

+44 (0)330 045 2105

Related expertise

Services

