Client: iStorage Yellow News
Source: Tech & Learning UK (Web)
Date: 05 March 2016
Page: N/A
Reach: 425
Value: 11

iStorage: Data security in education

The confidential nature of student and staff information means schools and other educational institutions are frequent victims of data breaches, as shown in recent research by the UK's regulatory body for data protection, the Information Commissioner's Office (ICO). Data security is an extremely important subject for the sector, as the loss of or unauthorised access to data can potentially cause significant harm to pupils, parents or staff, along with causing reputational damage and substantial fines.The ICO recently published a data security incident trends report, which revealed that the education sector saw 19 breaches in the last quarter, many of which were due to the loss or theft of an unencrypted data storage device. Furthermore, a survey undertaken at BETT 2015 by iStorage discovered that while 96% of respondents regularly carried portable storage devices such as USB sticks, portable hard drives, CDs and DVDs, only 28% are currently encrypting this data and over a third admitted to having lost a portable storage device that contained personal or institutional data.Under the terms of the UK Data Protection Act 1998, organisations handling personal information about individuals have legal obligations to safeguard that data. According to the ICO, all data kept on electronic media within educational institutions should be kept secure, encrypted and logged in order to keep track of any theft or loss. Where theft or loss does occur and encryption has not been imposed, enforcement action may follow which could be a fine of up to £500,000. The ICO also stresses the need to be particularly vigilant with portable devices such as USB flash drives and external hard drives.There are many educational organisations failing to implement safe technologies, evidence of which can be seen in the incidents of data loss catalogued on the ICO website. The importance of having strong security procedures in place when securing sensitive material cannot be underestimated.There are some simple steps that can be undertaken to ensure compliance:Be clear on policies – Ensure all staff are clear on what data security policies are in place and what their responsibility is. There can often be a 'it's not my responsibility' culture, so providing clear written guidelines will help staff be aware of what they are accountable for.Recognise the data type - Personal data is information which relates to an identifiable individual such as names, dates of birth and addresses. Sensitive personal data is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences. Although data protection principles relate to all data, there are greater legal restrictions on sensitive personal data and it requires additional security measures.Encrypt all data – There is a wide range of encrypted portable solutions such as USB flash and hard drives available today offering a combination of physical and digital security measures. These features include multi-digit PIN access via on-board keypads, military grade real-time data encryption and anti-brute force hacking capabilities, which together deliver the most robust, 360-degree portable data security solutions.

Unattributed[sourcelink]http://www.techandlearning.uk/download/istorage-data-security-in-education/
[/sourcelink]