wardhadaway lawfirm

June 2017

Ward Hadaway – Lawyers for Education

Insight: Education

Your monthly education sector news roundup

In this issue:

Information security and the education sector

Cyber security in education – lessons learned from the WannaCry ransomware attack

Upcoming event: General Data Protection Regulation – are you ready?

Monthly policy and guidance quick read

Insight: Education

Round up

Welcome

Welcome to the June edition of our monthly newsletter for those working in the education sector. We hope you will find this a useful summary of latest developments in schools, further and higher education and the training and apprenticeships arena. If you have any comments on the format or want more detail about a particular subject, please do not hesitate to contact any of us.

Information security and the education sector

What's new?

The recent global ransomware attack which affected the NHS has made cyber security headline news in the past few weeks. The attack has served as a wake-up call to organisations in various sectors to review their cyber security safeguards. However, cyber security is just one element of information security, which encompasses the strategies for managing the processes, tools and policies to prevent, identify, document and counter threats to both digital and non-digital information. In this month's newsletter we provide an overview of the importance of information security in the education sector. This discussion is set in the context of the implications of the forthcoming General Data Protection Regulation (GDPR), set to become law in the UK in 2018. Lastly, the specific concern of safeguarding against the risks of cyber-attacks is outlined.

What is at risk?

The Information Commissioner (ICO) is proactive in warning the education sector to be particularly vigilant regarding information security and regularly updates its guides explaining organisations' responsibilities. The ICO's reports on data security incident trends show that in the third quarter of 2016, there was a 40% increase in reported data security incidents in the education sector. Reported incidents this year such as the Department of Education ransomware alert in January and the theft of Edmodo users' details last month are a stark reminder of the need to remain alert.

Schools, colleges and universities handle large volumes of sensitive information which could cause serious harm if they were to end up in the wrong hands. Common vulnerabilities in information security in the education sector are:

PERSONAL DATA

The storage, transmission and transportation of the data of students and staff (contact details, addresses, dates of birth, medical history, banking and financial information etc.) presents risks. Systems must be robust and provision made to ensure that only authorised and appropriately trained personnel have access and handle the confidential information.

INTELLECTUAL PROPERTY

The theft of intellectual property such as patents awarded to professors and/or students and scientific and technological research carried out by a research facility is a threat which applies particularly to higher education institutions. Attackers view these as desirable assets to hold for ransom from the organisation concerned.

Insight: Education

Round up

UNPROTECTED WEBSITES

Denial of service attacks, which target unprotected websites, are increasingly being used in the education sector to make it difficult or impossible for legitimate users to gain access.

MOBILE DEVICE SECURITY

Risks to network security are created by the various devices (mobiles, tablets and desktops) used by staff and students, which are all competing for access.

The GDPR

Safeguarding must be considered in light of the GDPR which is set to bring about the biggest reform to information security since the Data Protection Act 1998. Brexit will not affect the application of the GDPR which will come into force on 25 May 2018. The legislation will bring significant changes to the sharing and controlling of information. The changes which educational institutions will need to be aware of are highlighted below:

» New rights

Right to be forgotten

Individuals will be able to request the deletion or removal of personal data, including that which is published or processed online. This could potentially become an area of contention between PhD students and universities. Students may request the removal of information; universities on the other hand will want the benefit of research students' profiles and research information for marketing purposes to build prestige and bolster funding opportunities. Institutions may need to turn to intellectual property arguments to challenge the removal of such content.

Data portability

This right is commonly referred to as subject access and is usually used by individuals who want to see a copy of the information which an organisation holds about them. The GDPR requires that this must be given in a format which makes it easy for a computer to read, for example, in a spreadsheet. Organisations should consider the implementation of processes to handle and document requests in a consistent manner.

» Conditions for processing data

The GDPR introduces six new conditions for processing data:

- Explicit consent given by the individual;
- To fulfil and prepare a contract;
- Existence of a legal obligation (other than a contract);
- To save a person's life or in a medical situation;
- To carry out a public function; and
- Some other legitimate interest (excluding public authorities).

Where data is sensitive (e.g. relating to race, religion, health status etc.), an additional justification for processing the data is required.

Insight: Education

Round up

» Consent

The GDPR takes a new approach to consent. Consent must be explicit. Silence does not amount to consent and "tick to opt out" boxes are no longer acceptable. Rather, specific "opt in" boxes will need to be used. This could have an impact on the marketing approach of universities, which use data to promote products and classes to university students and in communications with alumni.

» Additional principles

Six new principles are introduced by the GDPR:

- Data collection must be fair and lawful;
- Data can only be collected for a specific purpose and is limited to that purpose;
- Data collection must be necessary and not excessive for its purpose;
- Data must be kept accurate and up to date;
- Data should not be stored for any longer than necessary; and
- Data must be kept safe and secure.

A data controller must be able to show that they have complied with these principles. This requirement reinforces the need for educational establishments to have clear compliance structures, with clearly defined roles and regular training given to staff.

» Large organisations

Large organisations will need to appoint data protection officers. This affects organisations processing more than 5,000 personal records per year, those employing 250 staff or more and all public sector organisations. This brings risk management to the fore and auditing information will need to be held by organisations. In addition, universities will have to consider the potential implications of processing the data of international students as organisations are potentially liable for data which is transferred out of the European Economic Area.

Data protection breaches can result in reputational harm to educational establishments. It is expected that Ofsted will continue to heavily criticise schools which breach data protection legislation. Moreover, privacy literacy is increasing in parents and students and they expect schools, colleges and universities to be compliant. All establishments must also be aware of the possibility for individuals to bring compensation claims through the courts.

The potential financial harm of non-compliance is set to heighten under the GDPR. Currently under the Data Protection Act, non-compliance can result in fines of up to £500,000 imposed by the ICO. However, failure to comply with the GDPR could result in the data controller (and anyone else involved in the chain of data handling) hit with fines of either 4% of turnover or €20 million, whichever is the greater.

Insight: Education

Round up

What to do next

KNOW WHAT DATA YOU HANDLE AND PROCESS

An important first step is understanding what data is collected from students, parents, staff, management and other stakeholders, and being aware of what that personal data is being used for.

↓

PLAN FOR COMPLIANCE

Those involved in governance and management of educational establishments must engage in discussions to determine:
(1) how compliance with the data protection principles will be demonstrated; and
(2) whether a data protection officer needs to be appointed.

↓

REVIEW POLICIES

A review of existing policies is essential to determine the steps necessary to comply with the forthcoming changes, including the new right to be forgotten and the requirement for data portability.

Cyber security

40% increase
in reported cyber security incidents in the education sector.

(ICO, 2016 - Q3)

1 in 3 universities
face cyber attacks on an hourly basis.

(VMware, 2016)

43% of universities
have had exam results infiltrated.

(VMware, 2016)

Insight: Education

Round up

Increasing reliance by all educational establishments on computers and connectivity makes the lessons to be learned from the WannaCry ransomware attack, which affected the NHS, all the more significant. Generally speaking, the risks of cyber-attacks increase in line with the range and level of education provided by an organisation. However, no establishment is immune from attack. It is important for every organisation to have protection in place, which is reviewed regularly along with a contingency plan.

Ransomware is a type of malware which has been used by hackers for many years. Its effect is the locking or encryption of files, which makes them inaccessible to users. Emails, social media links and unsafe websites are potential entry points for malware into a system. Files will either be locked or encrypted, requiring a payment before restoring access to files and to the system. Bitcoin, the anonymous digital currency, is the usual form of payment demanded by hackers. Of course, there is no guarantee that once paid the ransomware will be removed.

The level of protection that an organisation requires must clearly be appropriate to its size and the nature of the system which it operates. Nevertheless, there are some key messages which should be taken on board by all establishments, with a view to protecting against the risks of cyber attack:

- Ensure that anti-virus and anti-malware systems are adequate. Install updates as soon as they become available.
- Bolster security by ensuring that any systems which are connected or accessible from the internet but do not have to be are disconnected.
- Regularly back up data. This will mean that in the event of a cyber attack, your organisation will be able to restore to a ransomware-free system.
- Train all staff on the importance of cyber security. The people within an organisation are often the weakest link. Individuals must be aware of the ease with which malware can be uploaded and educated on the potential impact on the whole of the organisation.

Upcoming event

General Data Protection Regulation – are you ready?
Tuesday 11th July 2017, 8.00am – 10.30am, Ward Hadaway's Leeds office
Thursday 13th July 2017, 8.00am – 10.30am, Ward Hadaway's Newcastle office
The new General Data Protection Regulation (GDPR) is just a year away. The legislation sets new responsibilities in areas such as child consent, corporate governance and reporting of compliance breaches. So what does it mean for your Academy Trust or School and how should you prepare for its introduction? Our education specialist information law experts will discuss new General Data Protection Regulation and what it means for your Academy Trust or School.

Insight: Education

Quick read

Need to know – your policy and guidance quick read

Crown Commercial Service newsletter for schools and academies – May 2017

The Crown Commercial Service has published its second quarterly newsletter which provides updates to help schools and academies buy common goods and services. This issue includes information to take part in aggregated further competitions and quick links to live frameworks and pipeline.

For more information please click here.

Guidance: Accreditation of GCSEs, AS and A levels for teaching from 2017

The list of subjects being accredited for teaching from September 2017 has been updated to include Pearson 'A' level maths.

For more information please click here.

Guidance: School census: notepad entries for COLLECT queries

The Department for Education has updated its list of COLLECT queries and explanatory notes to help schools, academies and local authorities complete the 2017 school census.

For more information please click here.

Insight: Education

Meet the team

Meet the Education Team

As the evolving educational landscape continues to open up new opportunities and present challenges, you need to be confident that you are getting the right legal advice, at the right time and, of course, at the right price. Ward Hadaway's Education Team is recognised as a leading national player. Our friendly, commercial and pragmatic approach allows you to be reassured that you are in safe hands.

Whether you are a maintained school, academy, multi academy trust, free school, studio school or UTC, our team have an in-depth, up-to-date knowledge of the sector, making us ideally placed to offer the best possible advice to all those involved in the delivery of educational excellence for pupils, students and their communities. Click here to read about how we can work with you.

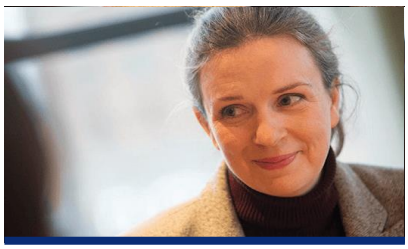
Your key contacts

Tim Care
Partner | Public Sector & Academies
E: tim.care@wardhadaway.com
T: 0191 204 4224

Frank Suttie
Partner | Commercial
E: frank.suttie@wardhadaway.com
T: 0113 205 6783

Paul Scope
Partner | Employment
E: paul.scope@wardhadaway.com
T: 0191 204 4352

Graham Vials
Partner | Employment
E: graham.vials@wardhadaway.com
T: 0191 204 4383



Fiona Wharton
Partner | Head of Charities
E: fiona.wharton@wardhadaway.com
T: 0191 204 4219

Alex Shiel
Partner | Head of IP/IT
E: alex.shiel@wardhadaway.com
T: 0191 204 4296