NW Security Group

The GDPR: Is your school, college or university compliant?

Best-practice for educational institutions

Table of contents

1. Foreword by Nigel Peers
Senior Consultant at NW Security Group

The rapid evolution of technology in recent times has fundamentally changed both our home and working lives. The rise of telecommunications and social media has enabled us to communicate with friends and business colleagues across the world, in ways we never thought possible. This has created the illusion of a global village; a term coined by Marshall McLuhan to define our increasingly interconnected nations and lives.

Within schools, colleges and universities, these technological advancements have also enabled networked physical security devices, such as CCTV, access control and intrusion detection systems, to communicate with each other. This means security and facility managers can better safeguard school buildings, and the students within them, so teaching staff can focus on their core responsibility; educating students.

But these technologies in turn generate vast amounts of data, which alongside the rest of the personal information an educational facility may hold regarding staff and students, has a value, both to the data subject and the malicious parties who may attempt to steal it. For that reason, one of the biggest shake-ups in history of data protection law is underway; the General Data Protection Regulation (GDPR).

The GDPR ensures all organisations are collecting, processing and storing personal data, or Personally Identifiable Information (PII), in a secure manner and with the data subject's permission. This should be welcomed in the education sector as, concerningly, data breaches are on the rise. Whether via cyber-attacks, accidental loss or poor data protection policies, the latest figures highlight that in Q3 2017 96 breaches were recorded, a rise of 68% from the previous quarter[1].

The ramifications of non-compliance have been widely documented[2]. If steps towards compliance are not taken, instances such as the hacking of a school's CCTV feeds, where images of staff and students were shared online[3], will become increasingly common, with educational establishments putting themselves at risk of fines and reputational damage.

It is therefore essential that all schools, colleges and universities achieve and maintain compliance with the GDPR. In this whitepaper, we discuss the findings of research undertaken by NW Security Group in the North West of England, in which we asked 500 head teachers, governors, IT, security and facility managers about their awareness levels of, and adherence to, the GDPR.

Nigel Peers, a qualified Data Protection Practitioner with full teacher training status, brings vast strategic security expertise as a previous co-founder of a successful workplace compliance training company, responsible for security site surveys, vulnerability assessments and Security Industry Authority (SIA) training courses. Working in close partnership with board and trustee-level stakeholders, Nigel is responsible for helping organisations understand the latest regulations and ensure risks, threats and vulnerabilities are correctly identified. Through strategic planning support, Nigel optimises security solution delivery from mitigation to implementation, risk and incident management to business continuity and recovery.

[1] https://ico.org.uk/action-weve-taken/data-security-incident-trends/
[2] https://www.itgovernance.co.uk/dpa-and-gdpr-penalties
[3] http://www.dailymail.co.uk/news/article-5432769/School-CCTV-systems-hacked-broadcast-online.html

2. Introduction

The EU GDPR establishes a legal obligation for schools, colleges and universities to have the correct policies in place to secure PII. However, the findings of our survey highlight that many educational establishments are still unclear of these requirements. In fact, only 22% of respondents felt their data protection policies were up to scratch, while 70% said that if they fell foul to a data breach, they wouldn't be able to evidence that the correct procedures were in place.

This is putting educational facilities at great risk of severe fines and reputational damage. As a security consultancy and training company, this is a problem NW Security Group became aware of while undertaking **Organisational Readiness Assessments** with schools, colleges and universities across the UK to help institutions meet their data protection obligations.

During those assessments, it was observed that although many facilities believed their processes were up to scratch, the reality was a somewhat different picture. Outdated policies and a lack of documentation were frequent failings indicating low levels of GDPR compliance throughout the sector.

Overall, the survey results highlighted a large amount of confusion regarding the regulations, with 64% of those who'd heard of the GDPR still needing more information. It is therefore clear that there is much work still to be done to propel educational facilities towards full compliance.

3. What constitutes a data breach?

Data breaches in the education sector skyrocketed in the first half 2017. There was a total of 118 successful attacks on educational institutions, a rise of 103% compared with the previous six months[4]. With such a dramatic and sudden increase, it's no surprise that education association EDUCAUSE named information security its top IT issue for 2018.

Despite this, NW Security Group's survey results highlight a surprising statistic: only 16% of educational institutions stated they had fallen victim to a breach. Upon first glance, this seems like an encouragingly low figure and in contrast to the sharp increases mentioned above. Could this statistic therefore be more accurately interpreted as: only 16% of educational institutions currently realise they have fallen foul of a data breach?

This is probably the case, and most likely due to a lack of understanding about what constitutes a breach. The term is not just a reference to cyberattacks; a breach can be something as simple as emailing data to the wrong recipient, verbally discussing PII in an open space, leaving hard-copy materials in plain view, or the loss or theft of unencrypted data.

That is why it was concerning to discover that almost a third of survey respondents (31%) didn't believe their employees and contractors were adequately trained in data protection. Employees are a school, college or university's first line of defence; if they can't correctly identify what a data breach is, the likelihood of achieving GDPR compliance is dramatically reduced.

Furthermore, 35% of institutions don't have someone on site capable of completing a Data Protection Impact Analysis (DPIA). This is an integral procedure to help identify and minimise data protection risks and ensure GDPR compliance. Most worryingly, however, when made aware of a breach, 14% of respondents said they'd completely ignore the issue and only 63% said they'd inform the relevant stakeholders.

This clearly highlights that all front-line staff that come into contact with PII must undertake the necessary **data protection training**, which will allow them to identify a breach and possibly even prevent one from escalating beyond control.

Only 5% of respondents have reported a breach to the ICO, and 84% don't think their facility has ever experienced a breach.

Despite 84% of respondents believing their facility has never experienced a data breach, 31% don't believe their employees and contractors involved in data processing activities are adequately trained to carry out their duties in compliance with the GDPR.

When being made aware that personal data and/or educational records had been obtained by an unauthorised individual, 14% of respondents would ignore the issue and hope the problem resolves itself and only 63% of respondents would inform the relevant stakeholders.

[4] https://edtechmagazine.com/higher/article/2017/12/education-sector-data-breaches-skyrocket-2017

4. Privacy by design
Ensuring data protection from the outset

To ensure adherence with the GDPR, educational institutions are required to implement a 'privacy by design' approach. This means that data protection should be a central consideration during the early stages of a project and throughout its lifecycle. This includes building new IT systems for storing or accessing personal data and developing privacy legislation, policy or strategies in other areas of a facility.

According to the survey, 43% of respondents ensure all technology, processes and policies are created with privacy by design in mind. Furthermore, 65% have a designated member of staff or outsourced service capable of conducting a DPIA in accordance with privacy by design.

These are positive steps that must be applauded. But while respondents may believe processes and policies are in place, the problem lies in a lack of documentation, as 70% said they couldn't effectively evidence privacy by design if they fell victim to a breach. The key lesson is that although the correct policies may be in place, if these are not documented a school, college or university will be deemed non-compliant. This of course increases both the risk of a fine if discovered by the ICO, as well as reputational damage.

This problem wasn't just identified within the survey findings. NW Security Group became aware while conducting Organisational Readiness Assessments that although many establishments believed best practice data protection processes and policies were in place, there was nothing to evidence the enforcement of these.

Documentation is critical to compliance, as the GDPR requires records of processing purposes, data sharing and retention to be kept up-to-date. NW Security Group advises educational facilities to ensure they complete the data protection process by not only developing robust procedures, but also recording these as written policies.

If they fell victim to a data breach, 70% of respondents didn't think they could effectively evidence 'privacy by design' to the Information Commissioner's Office, a critical element of GDPR compliance.

5. Technology with cybersecurity built-in

The best way to guarantee PII stored electronically is sufficiently protected is to ensure IT systems are secure, and that any technology installed on the network has been manufactured with cybersecurity in mind. In addition, it's important to choose integrators that understand the risks of installing security technology onto an IT network, especially for CCTV and access control systems that also capture PII.

Awareness is crucial. End users must know what to look for when seeking external help: Is the integrator Cyber Essentials accredited? Are they installing technology developed with a 'security by design' ethos? Are they utilising the technology in a secure way? These are the questions they must consider to guarantee technology is being used in a GDPR-compliant way.

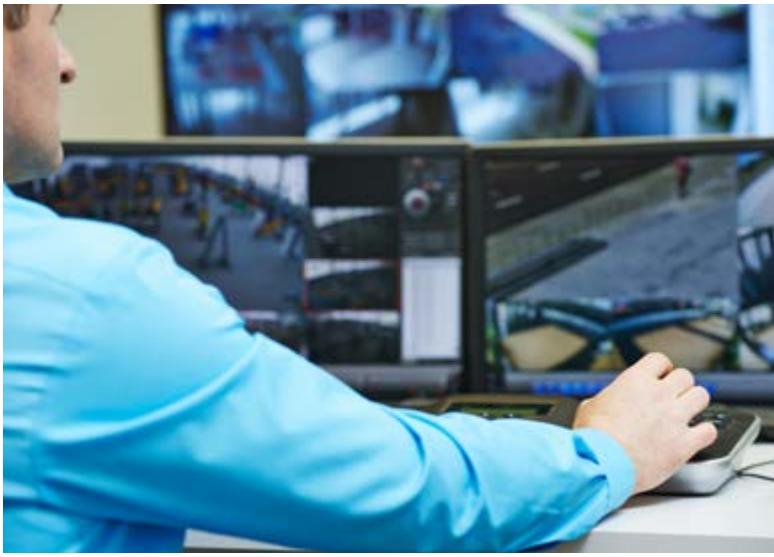
NW Security Group's survey found that 78% of respondents believe their facility actively promotes robust access control, and 86% of institutions implement a day-to-day visitor pass and booking-in system. Great news, aside from the fact that 51% of respondents said that the person responsible for the administration of an access control system is not trained in data protection.

True security requires collaboration between user and manufacturer, as systems are only as effective as the procedures in place to facilitate them, and the staff trained to use them. As well as having a secure network, it's critical that there's a well trained member of staff on site who's responsible for overseeing the system.

78% of respondents believe their facility actively promotes robust access control – 86% of institutions implement a day-to-day visitor pass and booking-in system for visitors.

But 51% of those responsible for the administration of an access control system are not trained in data protection.

In an emergency, 16% of respondents don't think they could produce a list of people that are on site.



6. Deploying a Data Protection Officer
Outsource or appoint internally?

A wide variety of organisations are required to appoint a Data Protection Officer (DPO) under the GDPR, including public authorities. Although uncertainty remains due to the interpretation of the regulation in this area, for those facilities that are not public authorities it is still considered good practice to appoint somebody responsible for managing GDPR compliance and reporting data breaches.

The DPO must be able to provide effective oversight. Yet finding someone with the relevant skills, experience and time to fulfil the duties of this role presents a challenge for many institutions across the education sector. That is perhaps why 22% of survey respondents are already outsourcing their DPO to qualified practitioners, a figure that NW Security Group expects to rise as more schools, colleges and universities seek to ensure GDPR compliance.

The outsourcing of this role is a logical solution. The DPO's duty is to monitor adherence with the GDPR, oversee data protection, raise awareness, train staff and run audits. Although this role can be filled by an existing employee, the GDPR stipulates there must be no conflict of interest and the DPO must have expert knowledge of data protection law. The security knowledge required isn't likely to be found among teaching staff, whose core focus is education. That is why an **outsourced DPO** could be the most effective, and cost efficient, resourcing option.

Only 22% of respondents who had heard of the GDPR felt their data protection policies and processes would be up to scratch.

7. Conclusion

These survey results clearly identify that the education sector is in a state of confusion regarding the GDPR. Awareness of the regulation is high, and in many cases the perceived levels of compliance is high, however, the reality is that with only 22% of respondents currently believing they are GDPR ready, more training is required to ensure and maintain compliance.

These findings are supported by NW Security Group's own experiences in the field. While conducting Organisational Readiness Assessments for education customers, it found that the most common issue was a lack of adequate documentation required for compliance. In many instances a facility believed it had the correct policies in place, but these were not written down or documented, and therefore could not be evidenced.

Undertaking an Organisational Readiness Assessment is the starting point to mapping out the journey to compliance – an essential tool for schools, colleges and universities to identify any gaps within their procedures that require being brought up to date. Once a roadmap has been set out, facilities will be able to maintain that status through ongoing training in order to continue adhering to good practices.

Having someone dedicated to ensuring and maintaining GDPR is crucial. An outsourced DPO could be the most efficient means, both in terms of cost and resourcing. This will provide the data protection and security experience needed, allowing staff to focus on their core job of education.

External experts are available to help schools deploy the best security systems, but technology isn't where data protection should end. You can go a long way with professional training and assistance to establish sound processes and procedures, keeping privacy by design at the forefront.

The survey

500 headteachers, governors, IT managers, security managers and facility managers within secondary and tertiary educational facilities in the North West of England participated in the research between 20 March 2018 and 23 March 2018.

To learn more about how NW Security Group can help you get on track to GDPR compliance, visit:

www.nwsecuritygroup.com/security-consultancy-training/gdpr

NW Security Group

About NW Security Group

Established in 2004, NW Security Group provides bespoke, all-encompassing security solutions that safeguard your daily operations. We combine technical expertise, consultancy and training to minimise risk and protect your people, assets and data. By working closely with you to tailor services that meet your exact requirements, we offer peace of mind and deliver long-term investment protection.

enquiries@nwsecuritygroup.com
www.nwsecuritygroup.com
Tel: 0151 633 2111