novatia

Helping to harness ICT excellence for education in a constantly evolving digital world

Novatia Note 017:

Ongoing Data Protection & GDPR Compliance for Trusts & Schools: the Data Audit

Key Points

- **GDPR compliance is an *ongoing* requirement**
- **Why do a data audit?**
- **What evidence of data scrutiny will the ICO expect to see?**
- **What should your data audit establish?**
    1. **What data is being held?**
    2. **Where did the data come from?**
    3. **Who is holding the data?**
    4. **Who are you sharing this data with?**
    5. **What are the data flows?**
- **Who can do a data audit?**
- **Need external advice?**
- **Get in touch**

The lead up to getting ready for the GDPR (General Data Protection Regulation) implementation in May 2018 created a flurry of activity within the Education sector.

Amongst the changes required by schools were the necessity of updated procedures and policies to demonstrate compliance, the appointment of data protection officers (DPOs), and third-party data processor agreements. Plus increased staff training & awareness.

Why do a data audit?

Going forwards, the key step to ensuring compliance is still to carry out a regular **data audit**. Understanding Education data and how it is being both handled, shared and stored, remains a top priority for senior leaders in order to minimise possible breaches. As a senior leader you should ask yourself, since your last **data audit.** have there been any:

- Organisational changes
- GDPR refresher training
- Support & development for DPOs
- New technologies & systems
- Data breaches
- Changes in third-party data processors

Don't forget, complying with this legislation, which is enforced by the Information Commissioner's Office (ICO), is an *ongoing* requirement. Any investigation by the ICO will scrutinise an organisation's commitment to data protection.

So, it's important that a **regular data audit** should establish…

What data is being held?

Data might seem obvious within your servers and management information system (MIS) but you need think about who else you are sharing this information with. E.g. other suppliers and integrators, such as any performance or

handwritten notes that contain personal information about people and annotated people files.

A survey to gather initial information is a good place to start. You need to ensure that you establish: **your purpose** for processing any personal data; any details about it e.g. current students or past; retention schedules and any technical security measures around that data e.g. how it's held, how it's encrypted, how it's accessed.

2. Where did the data come from?

You need to fully understand the multiple sources for your data. The most common sources in schools are either Local Authorities or teacher input. You need to be able to provide a data flow so that if the data is requested to be deleted you can ensure it is all captured or if there is a subject access request (SAR) you can track the data all the way through.

In the unlikely event that you don't know where the data came from then this needs to be flagged up as a gap in the data flow.

3. Who is holding the data?

By this we mean, *who is the responsible owner for that data?* E.g. For staff data it might be an HR Manager with this responsibility, however for student data it might be the Head of Year. Map out who 'owns' each source of data so that every record has an 'owner'.

Be aware that in schools records can be kept in a number of different areas. E.g. It is likely that data on parent governors is being held by two owners. Think about staff contracts too. Staff might be fulfilling a number of different roles. E.g. a teaching assistant with caretaker responsibilities might have personal data in two places, again with two different owners.

4. Who are you sharing this data with?

Here you need to think about software suppliers and solutions as well as any other organisations. You need to think about whether your information is up to date and whether all data is accounted for correctly. Now you need to provide a greater level of detail than ever before.

Be aware of data being held on local drives and laptops. Paper copies can hold key data too; GDPR isn't only about electronic data.

5. What are the data flows?

This is about establishing where the data items sit and where they go to. E.g. student data comes in from the Admissions Team and goes into the School's MIS. It then could go to organisations such as the Exam Board, Assessment Solutions, colleges. The purpose is to understand where the data is going and how long it is being kept in each area. Do each of these organisations have the right policies and systems in place to be compliant with their own GDPR as well as yours?

Who can do a data audit?

A data audit does require a certain amount of expertise; you can do this yourself, internally or bring in external support if necessary. An external company will find out more and dig deeper

than perhaps an internal auditor who might unknowingly overlook entrenched practices. Using the services of an external company also sends a much stronger message that your School or Trust is taking the matter of data protection seriously.

Finally, it might be easier to carry out an action plan that external consultants have recommended; handling data complexity will be one of the greatest obstacles to ongoing GDPR compliance.

If you have been contacted about an ICO audit, or would just like to know more about how Novatia can assist you with your own data audit please do get in touch. Alternatively, check out our website www.novatia.com or contact us on 01962 832632 or info@novatia.com.

We offer a FREE initial 30 minute phone consultation and would be happy to share some of our expertise.