novatia

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

Novatia Note 010:

Schools and GDPR—the crucial first step, your data audit

Key Points

- **Why do a data audit?**
- **Establishing…**

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?**

Why do a data audit?

On 25 May 2018 the new E.U. General Data Protection Regulation (GDPR) comes into force: as an Education Leader, understanding your current data position is an essential step in getting your School or Trust ready for compliance.

A data audit needs to be initiated from the top downwards, making it clear that this is a compulsory requirement for everyone in the School or Trust. That way you are more likely to uncover any hidden pockets of information being held by individuals or departments.

Changes to the rights of access to personal data under GDPR, with the possible increased demand for Subject Access Requests (SAR), means you need to scrutinise your data procedures *right now* – so you'll be able to comply efficiently with the changes next year.

A key component of GDPR is understanding what data is being held, where that data is and what the purpose of the data is. You also need to know *who* is holding it and if it's being held in the *right* way in order to minimise any possible breaches.

Here's what you should establish …

1. **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 tracking systems. These secondary systems may not sit on your school's server.

Data includes paper records and files that you have on students, staff, parents, governors. These are the ones that often trip people up. These might even include

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 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 GDPR compliance. If you'd like to know more about how Novatia can assist you with your data audit please see our website www.novatia.com or contact us on 01962 832632 or info@novatia.com.