GDPR Checklist for School Owners

Schools are regarded as 'data controllers' when it comes to General Data Protection Regulation (GDPR). This means that schools determine the particular ways, reasons and means in which they utilize the personal data in their control (primarily relating to their students and staff). As such, school owners must ensure that existing practices at schools or their school networks are GDPR compliant.

This checklist can be used as a starting point to ensure GDPR compliance.

1. Understand the principles behind GDPR

If you are processing personal data, or planning to process it, you need to understand the principles behind the regulation, or you need someone on your team who can do this for you. (If your organization/school network belongs to a public authority there will be a Data Protection Officer appointed). Understanding what is required under GDPR can help prevent problems and even fines due to non-compliance.

- [ ] Understand your obligations under GDPR
- [ ] Consult with a GDPR advisor or your Data Protection Officer

2. Assess if the processing is lawful

GDPR sets out conditions for being allowed to process personal data. You must ensure that the processing you are planning to do adheres to these conditions. If you are bringing in new technology or new purposes for processing data, you should do a Data Protection Impact Assessment. Processing of special categories (including health information) of personal data in general is illegal under GDPR (with exceptions) and we strongly recommend not processing this kind of data in the context of a learning platform.

- [ ] Define a clear purpose for the processing of data
- [ ] Ensure you have a legal basis for processing the data
- [ ] Make sure you don´t collect more data than required for your purpose
- [ ] Check that you don´t process (store) data for longer than needed for your purpose
- [ ] Do a Data Protection Impact Assessment

Read more about why the purpose of processing data is important.

3. Document the processing

This is often referred to as “Article 30 documentation”, as this GDPR article clearly states what records you need to keep for processing of personal data.

Create and review documentation of the processing activity, including:

- [ ] The name and contact details of the data controller
- [ ] The purposes for processing the data (see above)
- [ ] Categories of data being processed
- [ ] Categories of recipients of the data
- [ ] How long the data will be kept (retention policy)
- [ ] A general description of technical and organizational security (see Point 5)

4. Adhere to the rights of end users (teachers, students, parents, school administrative staff)

An important principle in GDPR is that people who have their data processed (known as data subjects) have rights under the regulation. While some of these rights depend on the nature of the processing, the rights are universal and also apply to students and their parents.

- [ ] Set up a communication channel for data subjects who want to exercise their rights
- [ ] Create and make available information about the data processing to the subjects involved in the processing. This includes:
    - Contact details for the controller
    - Contact details for the data protection officer (where applicable)
    - The purpose(s) for processing the data and the legal basis
    - Categories of data being processed
    - The categories of the recipients of the data
    - If applicable, information about transfer of the data outside the EU/EEA
    - How long the data will be kept (retention policy)
    - Records of the existence of data subject rights, and the possibility to lodge complaints against the processing
- [ ] Ensure that the systems you use can support you in complying with these rights. For instance, data subjects have a universal right to get a copy of their data that you are currently processing. Make sure your systems and/or vendors can support you in compiling such data if/when needed.

5. Implement/assess organizational and technical security measures

When processing personal data, you are responsible (together with vendors e.g. itslearning) for ensuring that there are appropriate technical and organizational security measures in place. The degree of how strict these security measures need to be is largely dependent on the risk to the data subjects should data be lost or compromised.

- [ ] Ensure that you have a system in place for regularly managing and assessing your security measures
- [ ] Create policies and procedures for how you require the system to be used and followed up on
- [ ] Train stakeholders in the processing in how to protect the data and the corresponding policies and procedures
- [ ] Ensure that there are appropriate safeguards to prevent unauthorized access to the data
- [ ] Ensure that your vendors offer appropriate security measures (see Point 6)

6. Assess suppliers

If you have a vendor (e.g. itslearning) involved in the processing of personal data, they will share some of the responsibility for the processing with you. But you are still responsible for making sure your suppliers are doing what is needed under GDPR. Above all, you need to make sure that no-one can bring new vendors into the process without assessing them first.

- [ ] Regularly assess the vendors' technical and organizational security measures
- [ ] Enter into a legally binding, GDPR compliant data processing agreement
- [ ] Train stakeholders in the processing in how to protect the data and the corresponding policies and procedures
- [ ] If a vendor processes personal data outside EU/EEA you might need to implement additional safeguards to ensure that the processing is lawful
- [ ] Implement a clear policy for how new vendors are selected

Ensuring that vendors involved in processing student data are in compliance with GDPR is a big challenge in schools and educational institutions where decision making often is decentralized. Read more about vendors involved in processing student data.

Since December 2020, itslearning has been a part of Sanoma Learning and has a Data Protection Officer (DPO) as defined under GDPR based in Finland. You can read more about our commitment to GDPR on our website:

https://itslearning.com/global/your-data-matters/gdpr

If you have any questions about GDPR and data privacy issues with regards to using itslearning, you can contact our DPO using the contact details listed here:

Riikka Turunen
Sanoma Media Finland Ltd
+35 89122 4791

privacyteam@sanoma.com

itslearning is Europe's largest provider of learning management systems for schools and universities. Built specifically for teaching, itslearning is today used by millions of people around the world. The company is headquartered in Bergen, Norway, with offices in 8 countries. Since 2019, itslearning has been part of the Sanoma Group.

Visit us at:
itslearning.com

itslearning AS, Solheimsgaten 7D, 5058 Bergen, Norway | T: 55 23 60 70