

Information security and privacy in Dutch schools

Using digital tools to assess student tasks requires teachers, school heads and policy makers to consider how to ensure a secure and valid use of student data.

Summary

As an organisation funded by the Ministry of Education, Culture and Science, Kennisnet guides Dutch schools to lay secure ICT foundations. Digital tools in education generate new questions around privacy, information security, exchange and ownership of data about learning. For teachers and students to effectively make use of evidence of learning, they need to be aware of these issues. Moreover, policymakers should set the right conditions. This case study describes the Dutch context regarding privacy issues and a working plan for making the right agreements with vendors/suppliers in this field.

Context

Secondary schools in the Netherlands have a certain degree of autonomy in the field of education. Students in the last two years of school have a more or less 'national' curriculum which contains 60% of the lesson plans (and which is centrally tested). The curriculum describes in detail what they need to know and be able to do. However, the educational interpretation is always up to the teacher including learning strategies. There is a final central exam in the Netherlands only for the last two years of secondary school.

On the other hand, the curriculum for the lower classes in secondary education and offer schools more freedom to make their own choices. Supervision is conducted by the [Inspection of Education](#), a body which is related to the Government but has an independent status.

[Formative assessment practices](#) are up to the school and take many forms. Many digital tools are used to adapt teaching and prepare feedback, from classroom polling tools to very extensive systems with rubrics and follow-up suggestions (some with the capability to generate automatic feedback).

Many schools use digital tools for formative assessment because these can record very specific information. Teachers see at a glance what has been learned, how it was scored and students still need to do. In addition, teachers have an "archive"; they can always go back and check how past work was done.

Assessment and digitization are becoming inextricably linked. But as attention for formative assessment grows, so does attention by policymakers at national level. Therefore, certain preconditions need to be fulfilled regarding privacy and information security, as will be described in this document in the context of The Netherlands.



A pilot study of formative assessment

The [Leidsche Rijn School \(NL\)](#) started running a [pilot study on formative assessment](#). Students Fedor, Milan, Souraya and Emma say: "Now I choose my assignments myself and I see that homework can also be useful."

The pilot started in year 3, as part of the Dutch curriculum for students at the so-called HAVO level (upper secondary school). All students receive feedback on the assignments they complete in class. They can also choose how they want to process the material, for example through visual material or with the textbook. In addition, all students speak to their mentor for 15 minutes a week. Then they talk about the student's progress, but also about how the student feels.

Nelleke Veels, a history teacher, explains that each student is given the opportunity to take a practice test before a graded test is taken at the end of a block. "Because we must meet the transition standard from year 3 to 4, each subject takes 4 graded tests per year. The practice test and the assignments together ensure that students know whether they have learned the material. "

The case

Challenges

Education is increasingly relying on ICT. The amount of information, including personal data, computer-click behaviour and (formal) test results, that are recorded by the various systems, is increasing every day. Therefore, it is important to have a good data administration not to lose vital information about learning.

The use of digital tools is easy to roll out, but schools should have clear agreements with suppliers/vendors. A major challenge is to get in contact and set conditions with the international suppliers of "free" products. Sometimes it is even impossible or very costly for a single school to arrange this. Privacy is less an issue if the tools can be used by students working with a guest account or "incognito mode" in the browser (e.g. Socrative, Kahoot!). But the moment a student must log in or enter personal data (such as name, date of birth or place of residence), schools need to be aware of the implications. An example of the complexity of logging in, in combination platforms like Google, Microsoft or Apple is described in the [following article in English](#).

Therefore, working with digital tools in formative assessment requires good agreements, keen awareness (and knowledge) of the potential risks and a professional culture and



awareness among teachers, students, school administrators and policymakers. It is the whole ecosystem which is responsible for students' *information security* and *privacy*.

Dutch organisations hold Google accountable for privacy risks

In education, more and more (personal) data is stored and exchanged digitally. It is important that this is done in a safe and responsible manner. Research commissioned by the University of Groningen (RUG) and Amsterdam (HvA) shows that there are privacy risks associated with the use of Google G Suite. The risks are in the collection of the so-called metadata by Google. Two organisations (SURF and SIVON) supported this research and are in talks with Google to ensure that Google removes these privacy risks.

The privacy risks have come to light through the so-called Data Protection Impact Assessments (DPIA) to Google G Suite. A DPIA provides insight into how data is collected, what is done with it and what the risks are. The Ministry of Justice and Security has had the DPIA exported to the enterprise version, and the University of Groningen and HvA have had research carried out on Google G Suite Education. SIVON, Kennisnet, the PO Council and the VO Council (the Primary and Secondary School Councils, respectively) are also involved.

Information security

Information security is to maintain coherent measures to guarantee a reliable provision of information. The information should not be modified (due to fraud or good intentions) or deleted, especially when it concerns important data such as test results (pass/fail) or learning statements (good/bad).

Information security focuses on the following aspects:

1. *Availability*: the extent to which data and/or functionalities are available at the right time. If a school wants students to use a specific tool, e.g., for a quiz, the tool should be approachable during that specific moment. The student should be able to log in, use the tool, answer questions. For instance, the server and tool should be able to handle many students logging in simultaneously.
2. *Integrity*: the degree to which data and/or functionalities are correct and complete. Consider, for example, adjusting an exam result. If the data is changed later, this can have major consequences.
3. *Confidentiality*: the extent to which access to data and functionalities is limited to those who are authorized to do so. For instance, parents should typically not have access to the data of other children. Schools should also consider whether students can view each other's test results.



Insufficient information security can lead to undesirable risks for the school, leading to financial damage and loss of image.

Information security violation in Stanislas School

The example of [the Stanislas School](#) in Pijnacker illustrates an incident that schools should avoid. The school received several messages from students, parents and teachers that inappropriate images or texts are visible during lessons run in the online conferencing tool Zoom.

The [school decided to immediately stop Zoom](#), after students were shown porn images during an online class. The Stanislas College has six different schools in this region. "In most cases, the images or texts seem to be shown by people who are not associated with the school and who have unlawfully accessed the class," the school writes in a letter to parents.

Privacy

Privacy is about personal data, which is any information that can directly or indirectly identify a natural person. Sharing of personal data must be regulated according to current laws and regulations. Therefore, this directly concerns policy makers and school leaders.

For example, [eye tracking](#) is a technology that creates new possibilities in education. Reading problems and reading strategies can be mapped and improved with targeted feedback and customization. But as with the use of biometrics or health data, it raises new privacy issues.

Eye tracking and formative assessment

Eye trackers are used, among other things, to improve (commercial) websites. This way, the designers can see exactly which parts of the website users are looking at and for how long. At one point, researchers decided to test this for educational purposes. But what purposes are these exactly?

Eye trackers can record where students look at on the screen during an assignment. With this data the teacher, for instance, can see what type of words students struggle to read. See also [this video](#) (in English), which explains how eye tracking can help with identifying reading difficulties (e.g., skipping words), and support students experiencing them.



Teachers can also track whether some elements on a page are too distracting, i.e., if the gaze drifts away from certain pieces of text. Designers can make use of such information to adjust and improve digital educational material.

New technologies like eye tracking, HoloLenses or virtual reality bring about new questions. However, policy makers should also be aware of how any digital tool records, processes and shares simpler data such as GPS, click behaviour and even document version history of students (e.g., at what time did a student complete a task). The word “processing” includes by law: collecting, recording, organizing, storing, updating, modifying, retrieving, consulting, using, disclosing by means of transmission, dissemination or any other form of making available, aggregating, linking, shielding, erasure and destruction of data.

Start with a risk analysis

Policy makers and ICT administrators who are responsible for privacy in school, need to think carefully about why a tool is used, by whom, what is the purpose and what information is recorded. The school must properly organize the use of digital tools and determine the specific suppliers to cooperate with.

This also means a school must properly inform parents and train teachers in the use of digital tools and discuss with students why certain tools are not suitable. After all, it is about the student himself. If he or she does not feel comfortable, this should be negotiable. It is highly recommended to start with a risk analysis when organizing information security and privacy.

Data privacy: Risk analysis in schools in Leiden

On May 25, 2018 the new data privacy law went into action (GDPR or *AVG* in Dutch). The 16 primary schools and 2 secondary schools of a school board in Leiden (called SCOL) also set to work on this. Melle Klamer, data protection officer (*FG* in Dutch) at SCOL and Frits Hekstroe, chair of the SCOL Executive Board, talk about their approach with a risk analysis as a starting point:

“We first had a risk analysis made and used it as a starting point for further work on our information security and privacy,” says Melle Kramer, data protection officer (FG) at SCOL.

Initially, we had set up a broad working group for this topic. We quickly concluded that it was more efficient to work with a small, decisive group. I then started working with the board secretary and a communications advisor. This was an agile group that was



able to quickly make progress with the 'red' points from the risk analysis. Those points were in 3 areas: policy, technology and behavior.”

Make agreements with suppliers regarding privacy

The **Schoolinfo** organization aimed at supporting schools in digitization, has done a lot of work in the Netherlands to **describe good tools** for schools and teachers who want to get started with digital tools.

If the school uses such digital applications, which include personal data of students and staff, then the school should make arrangements with the supplier. The school board should ensure that this information is stored securely and that it is not misused or hacked. **Kennisnet** has therefore developed two documents that schools can use to make good agreements with suppliers. Both documents can be consulted below for helping policymakers:

1. **[Privacy Agreement Digital Educational Resources \(3.0\)](#)**
2. **[Model Data Processing Agreement \(3.0\)](#)**

The new GDPR privacy legislation obliges the school to record agreements with suppliers about security and privacy in a so-called processor agreement. This contains agreements with suppliers - also called processors - about handling of personal data in the same way. These agreements have been extensively tested legally but might require adapting in the case of other countries. Kennisnet has also drawn up **a list of suppliers** who have signed the privacy agreement.

A roadmap for contacting suppliers

Step 1: Is the supplier already affiliated with the privacy agreement?

You can inquire about this with the supplier or consult the list of existing affiliated suppliers. If the supplier is not (yet) affiliated with the privacy agreement, invite them to do so.

Step 2: Request the processor agreement from the supplier

According to the GDPR, the school board must ensure a processing agreement. Request a completed copy from the supplier. As agreed, schools must receive a processing agreement from their supplier within 4 weeks of application.

Step 3: Check the processor agreement

Upon receipt of the contract, processors have to check that the contract was correctly filled, and the supplier did not adjust the original text.



Step 4: Agreeing and returning the processor agreement

Is the processor agreement correct? Then it can be signed by the school board. The competent authority is ultimately responsible for the privacy of students and employees.

Research - Evaluating and questioning our relationship with technology

Education futurist [Keri Facer \(2011\)](#) suggests that both educators and learners should be encouraged to understand and question their relationships with technology, and how information is being gathered and filtered on their behalf. Facer notes, "When applied to information filtering, as with our search engines, we can't simply think of our interaction with these systems as a process of 'using' them. Instead, they are playing an active role in shaping and managing our interactions." (p. 66).

The "appchecker"

Finally, teachers can sometimes be too enthusiastic and quick to adopt a new digital tool and not consider the personal data processed by the tool. Therefore, Kennisnet developed a self-assessment tool named [appchecker](#) (available in English). The tool is designed like an online form/checklist that asks the respondent the privacy-related points to have in mind when choosing a digital tool (e.g., "Does the tool ask you to fill in personal data?", or "Does it ask you to access parts of your smartphone or PC"). It also provides explanations about these questions. The tool ultimately aims to create more awareness by teachers and support schools in addressing information security. This tool will soon be available in English.

Research - Development of an ethical framework to guide decision making on use of educational technologies

[Olcott et al. \(2014\)](#) engaged with schools in Catalonia to analyse emerging ethical questions and choices related to the use of digital technologies, with relevance to other local and national contexts. They then developed a framework based on the Ethical Context Continuum (ECC) to guide decision making on the potential harm and/or benefits of different digital technologies to individuals and groups.

The framework sets out four principles for consideration by governments, companies, educators, private citizens and others:

- Training in the responsible, secure and ethical use of technologies must reach all members of society.



- Education is based on values, and education is provided in, with and from values.
- Technologies should be used appropriately (judiciously and respectfully), not just used.
- Individual and collective commitment determines the responsible and exemplary use of technologies (e.g., individual collective harm and/or benefit).

The authors suggest that complexity and potential ethical issues related to use of digital technologies in education is likely to continue to expand.

Conclusion

Dutch schools have increasingly become aware of information security and privacy. Consequently, schools aim to handle student data and test results carefully. The drafting of processor agreements is common. However, teachers might still independently look up tools on the internet and use them in their teaching without precautions.

The presented instruments and good practices from the Netherlands could be adapted to the context of other countries. At school level, it is also important to have good cooperation between the school board, a privacy officer (or the ICT administrator) and teacher.

Students and parents should also be involved in creating awareness, because they are a crucial part of the ecosystem. The goal is to have students ask critical questions about the use of a digital assessment tool in the classroom. Although there is progress to be made to reach that goal, the first steps have now been taken in the Netherlands.

