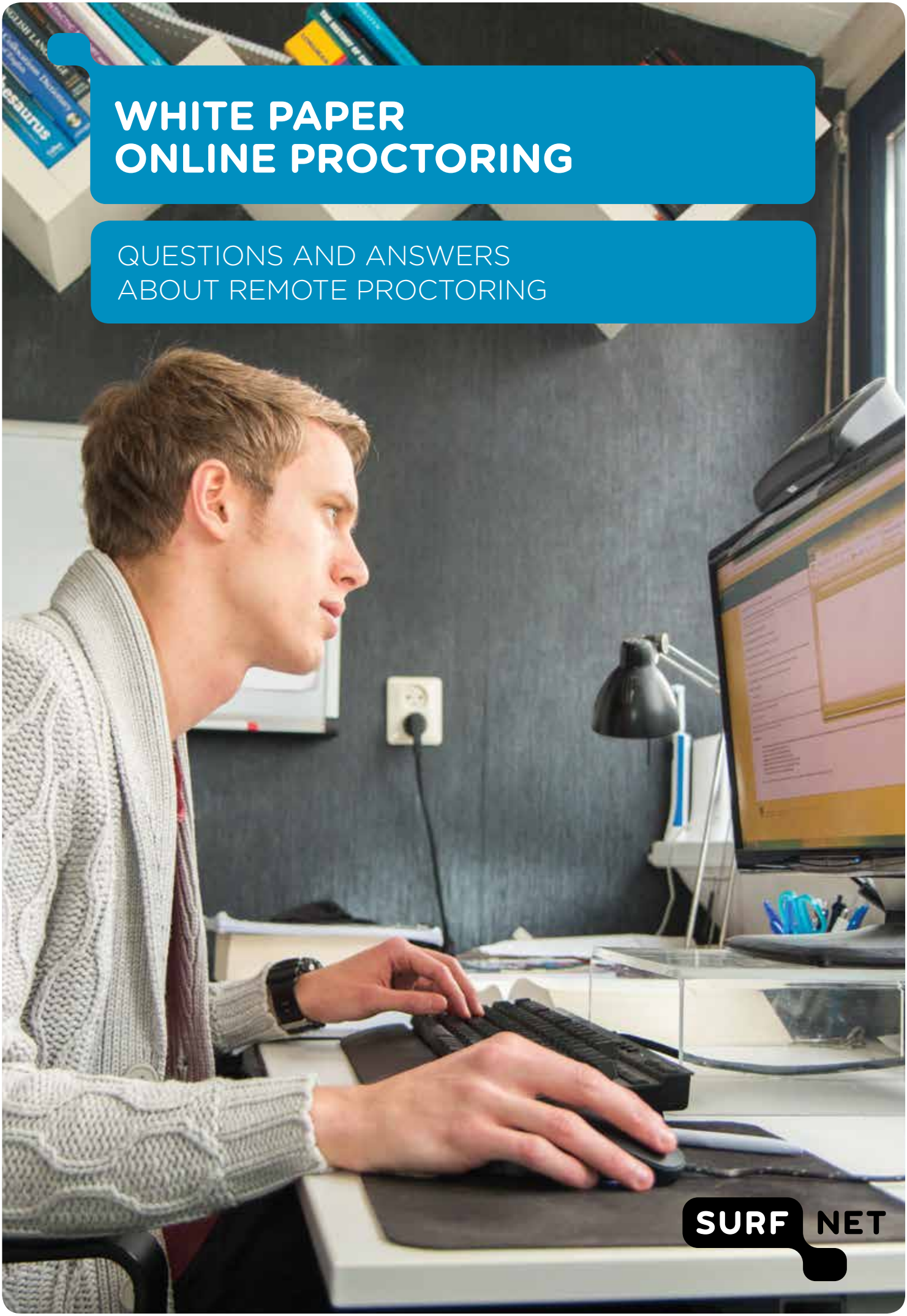
# WHITE PAPER
# ONLINE PROCTORING

QUESTIONS AND ANSWERS
ABOUT REMOTE PROCTORING



SURF NET

# FOREWORD

Online proctoring – or online invigilation – is increasingly being used in education (including higher education) in the Netherlands. It offers students the option to take tests remotely (independent of location[1]) in a secure and reliable way. In many situations, it can offer an ideal solution.

Examples include massive open online courses (MOOCs), students doing internships abroad but having to take an exam in the Netherlands, or international master's candidates who are admitted based on the results of an exam. Online proctoring can therefore be used to make the education process more flexible.

However, there are still many unanswered questions relating to privacy and the resilience of the various proctoring systems against fraud, for example. Scarcely any scholarly research has been done on these issues, and any practical experience has primarily been gained through small-scale experiments. Because of the rapidly changing market and the lack of research, it is difficult to gain a clear understanding of online proctoring. This makes it difficult for exam boards to assess whether or not it is a suitable resource to meet specific needs within their courses.

With this white paper, SURFnet wishes to provide a greater understanding of online proctoring and the issues that it raises. The white paper has three parts. The first part (sections 1, 2 and 3) is general in nature. Sections 1 and 2 describe what forms of online proctoring exist and what situations it is currently used in. The background to proctoring is also addressed. Section 3 covers the key issues that emerge in the use of online proctoring (privacy protection, security, anti-fraud measures and costs). The second and third parts of this white paper provide greater detail. Section 4 takes a close look at privacy protection, while section 5 looks more closely at security and anti-fraud measures. Section 5 also includes an assessment security selection tool developed by SURFnet, which can be used by exam boards to assess which exam resource would be suitable for their specific situation.

This white paper deliberately does not compare the various suppliers of online proctoring. The market is developing rapidly and suppliers are constantly adapting their products, which would quickly render any comparison out of date. Fortunately, there are plenty of overviews of suppliers and their offerings to be found online[2].

**More information on digital testing and online proctoring can be found on SURF's website. SURFacademy regularly organises meetings about these issues. If you have any specific questions about the topics covered in this white paper, please contact Lex Sietses, *lex.sietses@surfnet.nl***

1. Proctoring software is also regularly used within the institutions themselves. In that case, however, it does not constitute 'online' proctoring but rather a Bring Your Own Device (BYOD) solution or a computer lab at the institution itself. This white paper only looks at online proctoring where the exam is taken outside of the institution.
2. See Eduventures, for instance: *http://www.eduventures.com/2015/08/the-developing-market-for-online-proctoring/#watched* or *https://proctorexam.com/* (in Dutch) (check whether this is the latest version).

# CONTENTS

# SUMMARY

Online proctoring – or remote surveillance of exams – is on the rise. It is being used more and more in the USA, and Dutch educational institutions are also increasingly experimenting with it. Online proctoring offers opportunities a flexible education as well as international courses, but there is still a lack of experience with it – especially in the Netherlands. Because of this, exam boards and other stakeholders within study programmes find it difficult to decide whether to use online proctoring in their courses and, if so, how. They struggle with issues relating to fraud prevention and privacy.

In this white paper, SURFnet concludes that online proctoring can add a lot of value in specific situations. At the same time, the large-scale introduction of online proctoring would have a major impact on privacy. This raises questions about its desirability and whether large-scale use would be compliant with the existing legal frameworks. Furthermore, holding exams outside the controlled environment of your own institution introduces fraud issues. The key conclusions are set out below.

### The possibilities of online proctoring

Online proctoring offers a solution for specific situations. For example, online proctoring allows Wageningen University to offer an entirely online master's programme in which students can take their exams from anywhere in the world. Online proctoring also allows elite athletes to take exams while based at their training camp, and seriously ill students can also take exams from home.

In general, online proctoring makes it easier to hold exams flexibly in terms of time and location. Institutions currently consider it unrealistic to offer their students the opportunity to take exams at any time. Online proctoring makes this easier. It goes without saying that solutions of this kind require that each student is given a unique exam. This might be based on an item database containing many exam questions.

### Privacy and online proctoring

An important consideration when processing personal data is proportionality: does the end justify the means? Online proctoring has a major impact on privacy. Camera images fall into a separate category under the EU's Data Protection Directive: namely, that of sensitive personal data. For instance, camera images can be used to track medical data (e.g. 'wears glasses'), race and ethnicity. Consideration must be given to proportionality on a case by case basis, but large-scale use of online proctoring for all exams and for all students is almost certainly not proportional.

Furthermore, permission from students is the most obvious basis on which data may be processed. This permission must be given freely; a student must therefore be able to refuse permission without suffering any negative consequences. If students are dependent on their education institution, then we cannot say that their permission has been given freely. Institutions need to be very careful about this and may not in any way attach consequences to a refusal of permission. Online proctoring cannot therefore be made compulsory, and the institution must always offer the student a free alternative as well.

Institutions must also ensure that their request for permission is as clear as possible, and that it indicates what data will be processed, for what purpose that data will be processed, who will be able to access the data, how long the data will be stored for, and what will subsequently

be done with the data. This must be formulated clearly and be stated in the place where the student gives their permission. It may not be hidden, and may not be contained in a privacy statement. Finally, institutions must also take account of strict requirements for the storage and processing of personal data. It is also important to note that there are even stricter requirements placed on the storage and processing of camera images.

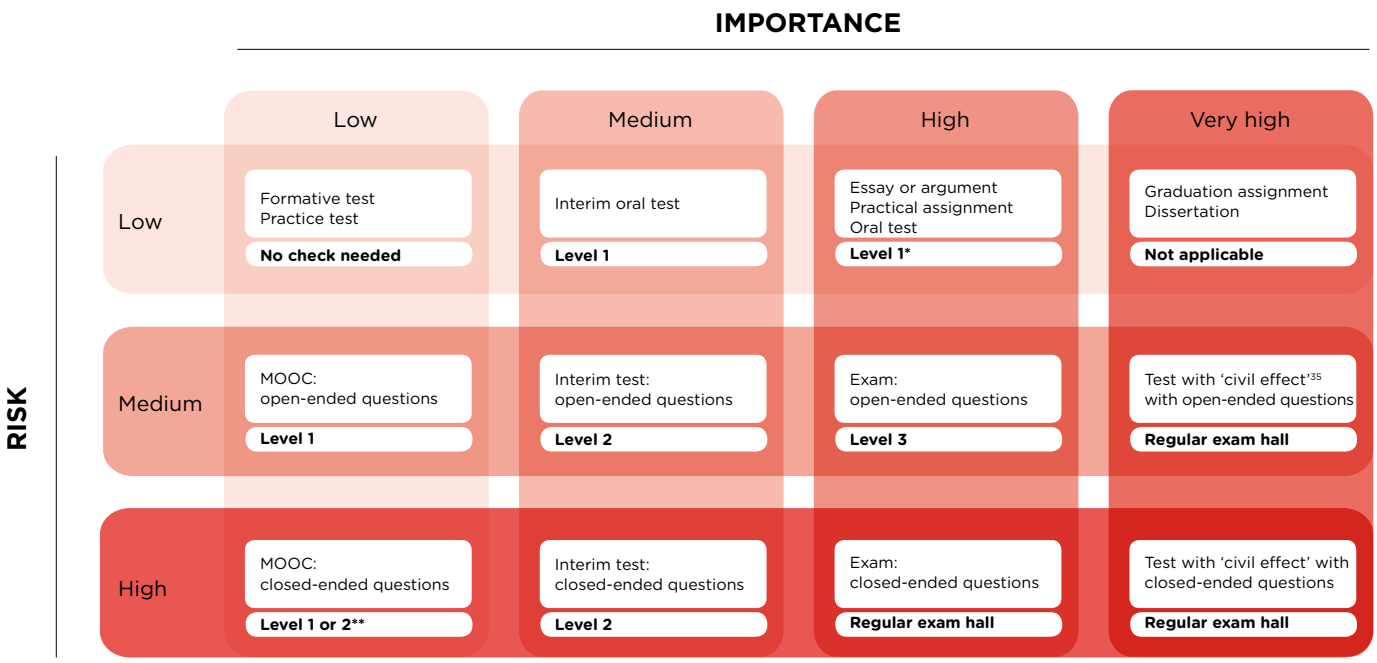
### Online proctoring fraud prevention

If the education institution has no control over the location where the exam takes place (a principle that lies at the heart of online proctoring), then online proctoring offers insufficient protection from fraud. Especially when exam questions are multiple choice, there are too many opportunities for fraud. SURFnet has therefore developed a selection model that helps decide which exams are suited to online proctoring. The assessment of whether or not online proctoring is suitable for a particular exam depends on two factors: the importance of the exam and the risk of fraud. The model is set out below with a brief explanation; further detail is provided in section 5.4.
The importance is determined by the (immediate) effect of the particular exam and the value that society places on the assessment. For instance, a weekly interim test is less important that the final exam for a module, as fraud during a weekly interim test has much less impact than if the final grade for a module is obtained by fraud. The risk depends primarily on the test format. Fraud is simply much easier in multiple choice exams than in exams that ask open-ended questions or oral exams.

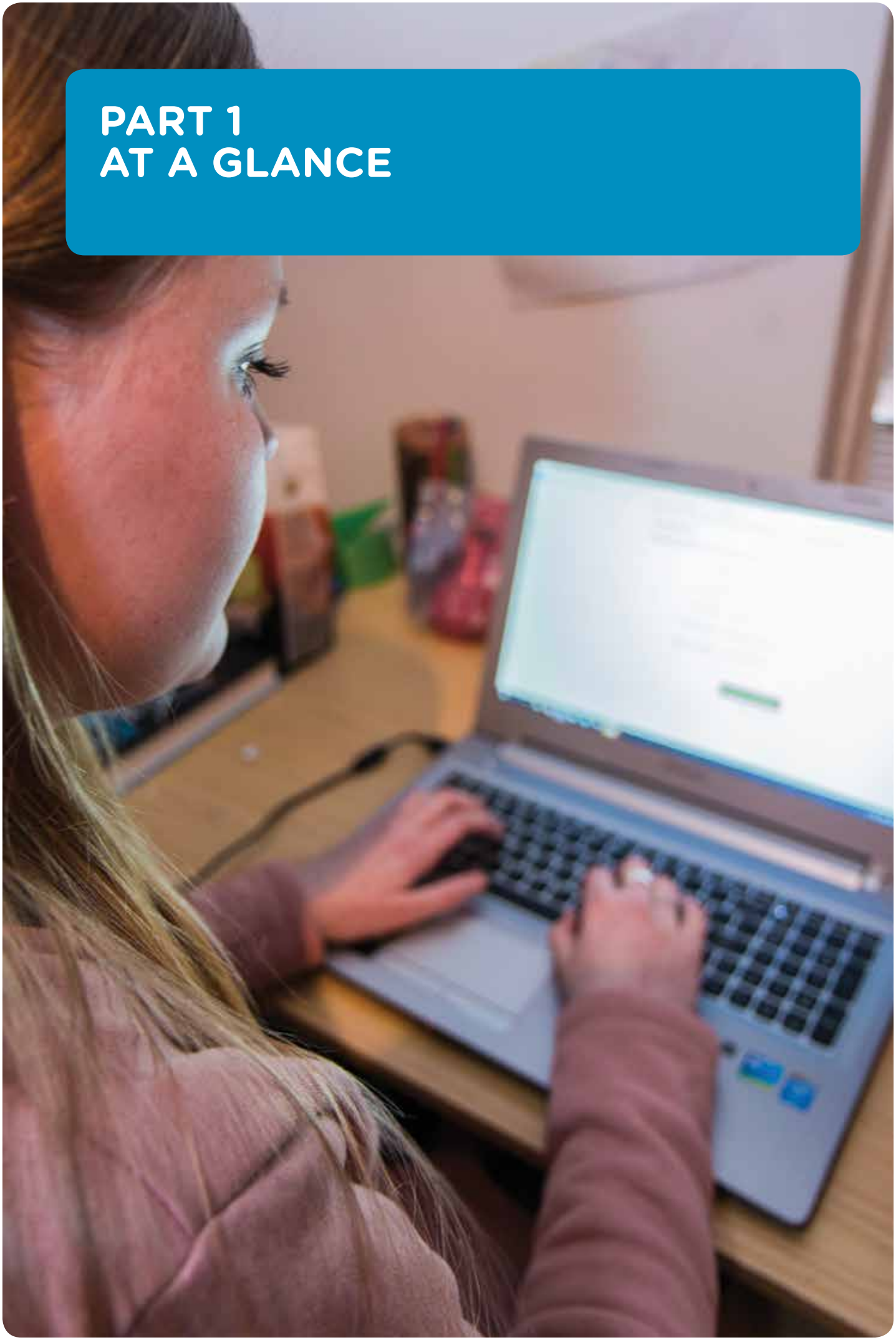
In online proctoring, three levels have been identified:
• *level 1:* screen capture and a single camera;
• *level 2:* screen capture and two cameras;
• *level 3:* full logging, screen capture, two cameras and only live proctoring or a recording.

This approach results in the model shown below.

### Assessment security selection model




* Naturally, online proctoring is unsuitable for essays and work performed over long periods of time. It is particularly suited to oral exams, for example.
** For MOOCs, this depends on the value placed on the MOOC.



# PART 1
# AT A GLANCE

# 1. WHAT IS ONLINE PROCTORING?

Online proctoring is a form of digital assessment that allows an exam to be taken from any location. Online proctoring software promises to allow students and course participants to sit their exams anywhere (e.g. at home) in a secure and reliable way. Monitoring software, video images and the ability to monitor the student's screen should prevent them from engaging in fraud.

The exact form of online proctoring varies from supplier to supplier, but we can identify three main categories: live proctoring, in which proctoring takes place during the exam; exams being proctored at a later date based on images and logs; and automated proctoring where the software is responsible for part of the detection. The key pros and cons are set out for each category.

## 1.1 Live proctoring

Live proctoring is the oldest and best-known form of online proctoring. It is the form that most closely resembles the real-world exam hall, with a proctor monitoring the exam remotely. The number of exams that a single proctor can follow varies depending on the chosen method. The more screens a proctor has to follow, the fewer exams can be monitored at the same time. The proctor can intervene during the exam, just like in an exam hall. For instance, during an open-book exam, they can ask the student to shake out or show their book to prove that there are no notes or crib sheets hidden inside.

The biggest drawbacks of this form are its limited scalability and the need to schedule the exam in advance. The student cannot simply log in and start work as soon as they feel ready; instead they need to schedule a time a few days in advance in order for a proctor to be available. The capacity of the system is determined by the number of available proctors.

## 1.2 Subsequent storage and verification

This commonly used form of online proctoring saves the camera images and logs for the proctors to review the (sped-up) video at a later time. Based on the images, they will assess whether or not any fraud was committed during the exam. The greatest benefit of this form is that students can sit the exam whenever they are ready. They can log in straight away and start an exam without having to schedule it in advance. Another benefit is that this form is easily scalable and can cope with large simultaneous exams. Large numbers of students can sit their exams at the same time, and the proctors can then assess them over a longer period. This is not possible with live proctoring.

The drawback is that a proctor cannot intervene during an exam, meaning they cannot tell the student that a certain action is illegal. It is also not possible to intervene if the camera is incorrectly positioned and the proctor does not have a full view of the desk. This would not be a problem during live proctoring, but in the case of an exam that was only reviewed at a later date, the test would have to be declared invalid.

### 1.3 Automated proctoring

In automated proctoring – which is growing in popularity – proctors no longer monitor (or review) the entire exam. Instead, the software identifies moments where there is a possibility of fraud. For instance, whenever other software is opened, the student looks away, or another person is detected in the room. The proctor is alerted to events of this kind, and they can then review the specific moments to assess whether fraud has actually been committed.

Automated proctoring makes the proctoring process much more efficient and saves a lot of time, as not all images and logs have to be reviewed. This also makes it a very scalable solution. One of the disadvantages is that if students know how the software works, they will be able to evade the fraud prevention measures more easily. By contrast, a human proctor remains unpredictable for the student because it is impossible to be sure what they are monitoring at any given time. Another drawback is that the software easily produces *false positives* (i.e. reports innocent events as potential fraud).

Online proctoring allows a single proctor to keep an eye on multiple students.

# 2. THE POSSIBILITIES OF ONLINE PROCTORING

Online proctoring holds the potential to make education more accessible and more flexible – especially for online and international education. However, there are also risks and doubts about its use. This section describes the key reasons to use online proctoring. The following sections then take a closer look at some of the issues involved.

## 2.1 International education

Increasing numbers of educational institutions are introducing open and online courses that can be followed from anywhere in the world. They vary from short online courses to entire master's degree programmes. Asking students or course participants to fly to the Netherlands for every exam is, of course, not an option. Institutions could work with international assessment centres or Dutch embassies to organise exams abroad. However, this is not ideal. It is sometimes very expensive, not easily scalable and not always a suitable solution in all countries. Online proctoring may offer a solution in this international context, where students live in all kinds of different locations (and countries).

### A fully international master's specialisation

"There are currently 25 students following the master's specialisation in Nutritional Epidemiology and Public Health entirely online. This 4-year part-time online master's programme leads to the same award as the regular 2-year full-time on-campus master's programme.

When offering a programme entirely online, it would not be appropriate to force students to come to the Netherlands to sit their exams. That's why we use online proctoring to make this possible. It also works well in the regular examination process. Where a lecturer would normally set the computer lab up for an exam, we now make the online environment available.

We see online proctoring not as a replacement for all on-campus exams, but as a great solution for specific situations. Alongside this master's programme, online proctoring is now being used for decentralised selection on the Netherlands Antilles, and we also have plans for students who are doing internships abroad or for elite athletes who have to attend a training camp."
**Rolf Marteijn, Wageningen University**

## 2.2 Flexibility in terms of time

More and more institutions are aiming to put students at the centre of their educational offerings instead of basing them on a fixed curriculum. This is also what the students themselves want[3]. Furthermore, students are not always ready to take their exams at the same time. While one student may have mastered the material in half the available time, another person may need additional time. Offering exams at any time is unfeasible with paper-based exams because exam halls and proctors would have to be available at every moment of the day. Online proctoring provides options here, allowing students to sit their exams when they are ready.

3. *http://www.lsvb.nl/actueel/rapport/lsvb-introduceert-de-flexstudent*

### 2.3 Flexibility in terms of location

Institutions want to be able to offer education not just at any time, but also in any location. This impulse is strongest with courses aimed at international students[4], but is also occurring more frequently for domestic education within the Netherlands. This is particularly true for part-time studies and work-study programmes, because students following this kind of course will be on campus less.

### 2.4 Different exam types

A common misunderstanding is that online proctoring is primarily or even only suitable for multiple choice exams. This is incorrect: online proctoring can be used to support any digital exam format. The use of webcams also offers other options, e.g. allowing handwritten notes to be taken into account when marking exams. The student can show them to the webcam and the examiner can then assess the scanned version.

## What students think of online proctoring

"The Dutch Student Union (LSVb) sees online proctoring as an interesting development. This form of assessment offers new opportunities and makes education accessible from around the world. In a world where internationalisation is playing an increasing role and education can also take place remotely, technological developments are inevitable. However, experimenting with this form of assessment also brings a number of risks. The sensitivity to fraud of this form of assessment remains a large risk which cannot be entirely eliminated, even when all the available countermeasures are applied.

The video material is also assessed by a third party, which seems to reduce the role of the exam board. This raises the question of whether verification can be guaranteed, and how this is supervised. Finally, the LSVb firmly believes that digitisation should take place as a complement to classroom-based education, which should continue to play a primary role. Interaction among students and between students and lecturers is essential in higher education."
**Stefan Wirken, Dutch Student Union (LSVb)**

---

"The ISO finds it very important that learning and exams should take place at any time and in any place. Proctoring is a good way to enable students to sit exams at home, and it makes it easier to allow students to decide for themselves when to take their exams. Because the student does not need to wait six months for an exam, there is no delay in their studies. However, it is important that the student receives proper guidance and that students still come together so that the student community continues to exist.

Despite the benefits, there are a number of risks posed by the use of online proctoring, specifically with regard to privacy and susceptibility to fraud. Institutions will come into possession of even more sensitive personal information relating to their students. As soon as that information is used wrongfully or is made public, both the student and the institution will face big problems. Another risk is that there is online proctoring can be sensitive to fraud. After all, it is easier for students to commit fraud in their own bedrooms than in an exam hall. Overall, the ISO therefore considers online proctoring to be an interesting development and sees opportunities to test it through pilots. It will primarily be a positive addition for students that need it, but it is not suitable as a universal solution."
**Simon Theeuwes, Interstedelijk Studenten Overleg (ISO)**

4. This refers to studies where students are spread around the world and follow the programme online, meaning it would be unrealistic for students to sit exams on campus.

# 3. ISSUES WITH ONLINE PROCTORING

This section examines the key issues raised by online proctoring: privacy protection, security and anti-fraud measures, and their associated costs.

## 3.1 Privacy protection

Online proctoring involves the processing of personal data: i.e. data that directly or indirectly identifies students. The Dutch Personal Data Protection Act (WBP) sets strict requirements for the processing of this data – for example in terms of requesting permission, informing students and securing the stored data. Section 4 looks at this in closer detail and offers guidelines that institutions can use to develop suitable tools.

**Section 4** What does the law say about privacy?

The key points of the WBP are:

- **Permission**
  Processing personal data requires a statutory basis (a condition that must be met in order for the data to be processed). In the case of online proctoring, this legal basis is almost always permission. The student must be capable of giving their permission freely, meaning that they must be able to refuse permission without suffering any consequences. In the case of regular education[5], therefore, online proctoring cannot be made compulsory; a free alternative must always be offered.

- **Information obligation**
  Before a student is asked for permission, they must be properly informed about what they are giving permission for. Having students check a box alongside a general phrase such as: "I grant permission for online proctoring" is inadequate, even if there a privacy statement elsewhere containing further explanation. The text used to seek permission must be sufficiently specific. One example of such a text is "I grant permission for key logging and the making of video recordings and screen captures from my PC. These images will be stored for a period of ## weeks. The proctor of <company X> and my examiner will receive this data in order to assess whether I have taken the exam in accordance with the rules. Please see our privacy statement for more information."[6]

- **Specific purpose**
  Personal data may only be used for the purpose for which it was obtained and for which there is a statutory basis (usually permission). Consequently, data from the online proctoring system cannot be used for learning analytics.

- **Sensitive personal data**
  The term 'sensitive personal data' is used to refer to data relating to someone's health, ethnicity, sexual preferences, political preferences and religion, for example. This data may not be collected or used without explicit permission and only where absolutely necessary.
  Online proctoring almost always involves the processing of sensitive personal data, such as identifiable heritage or ethnicity. Another known problem is the scanning of identity documents, on which the citizen service number (BSN) may not be visible. The requirements imposed on obtaining permission and storing this data are therefore more stringent.

5. The law is most stringent for publicly funded education. For MOOCs and optional modules, for instance, the student may choose not to take the course of module.
6. It is important to seek separate permission for any sensitive personal data obtained using camera images.

## Privacy in practice at TU Delft

"The Dutch Personal Data Protection Act requires us to seek permission from students prior to enrolment for a course before we can use online proctoring. Because we are still actively growing our online education offering and the exact form of assessment has not yet been decided in all cases, we ask all our online students for permission to use online proctoring – regardless of whether or not it will actually be used for that specific course.

Lecturers wanting to use online proctoring and the relevant exam board must be well-informed about the legal requirements, meaning that lecturers must always offer an alternative form of assessment or proctoring. This alternative must in turn meet the requirements of the exam board. In other words, there must always be an effective plan B."
**Meta Keijzer-de Ruijter, TU Delft**

### 3.2 Security and anti-fraud measures

**Section 5** How reliable is online proctoring?

Combating fraud is an important topic that attracts a great deal of public interest. Exam boards want to be able to stand behind every diploma they issue. Combating fraud already presents a challenge even in a regular exam hall, and it becomes even more complex when using digital means of assessment, such as online proctoring.

It is generally acknowledged that regular exam halls are not 100% secure. However, educational institutions and exam boards have a lot of experience in using regular exam halls, and are thus capable of making a relatively good assessment of the associated risks.

However, they have not yet built up the same level of experience with online proctoring. Many institutions wanting to use online proctoring will have to make their own assessment of how secure the solution they want to use is. A complicating factor is that each supplier uses different methods and technologies, so the experiences of one institution may not always be directly applicable to other institutions.

## Students carried out a security audit

"At the University of Amsterdam (UvA), we have already held around eight hundred exams using online proctoring software. We are very satisfied with the results. To follow up, we wanted to investigate how the software could be used in regular education, and so we decided to start the SURFnet 'Online Proctoring' project.

This project aims to investigate the security of the software, whether students can (easily) commit fraud, and whether the students' privacy is guaranteed. We gave the assignment to four IT students who specialise in hacking systems. These students carried out a small-scale security audit to assess whether students are able to commit fraud and whether any privacy issues emerged. They identified various issues that do indeed point to security and privacy issues. It was agreed with the supplier that they would start by tackling a number of these problems and that a second security audit would be performed to assess whether the problems have been solved.

It is likely that not all of the problems will have a solution. UvA now has to assess whether the risks are acceptable for UvA, bearing in mind that the regular exam hall is also not 100% fraud-free."
**Guusje Smit, University of Amsterdam**

Section 5 looks extensively at possible ways to commit fraud and how proctoring software attempts to prevent it. Based on this, the following conclusions can be drawn:

- Fraud involving manipulation of hardware or software can *usually* be detected. However, this often has far-reaching implications for student privacy.
- As soon as a student has developed software to make it possible to commit fraud, they could pass it on to a large group of students in the blink of an eye. This scalability is totally different in a regular exam hall where fraud is (almost[7]) always an individual activity.
- If the education institution does not have any control over the space where an exam is held, fraud can be committed in ways that are (almost) impossible to detect.
- With a little creativity, the list is almost endless.[8] Section 5 discusses a selection of possible opportunities for fraud.

Both online proctoring and proctoring in regular exam halls come with risks attached. Fraud is possible in both situations, but there are also differences. A regular exam hall always offers a higher maximum level of security. Online proctoring has inherent limits due to the nature of the system. The very advantage that an exam is no longer limited in terms of place also means that the education institution cannot control the environment where the exam takes place. Control mechanisms such as webcams reduce the risk, but do not eradicate it entirely.

Does this mean that online proctoring is useless as a means of organising exams? No, online proctoring is useful as a resource used to facilitate the organisation of exams in certain situations. However, it is important to make a well-founded decision that weighs both the importance and the risk of the specific exam, as well as the benefits.

Section 5 takes an in-depth look at possible ways of committing fraud and how online proctoring can offer protection from these. Furthermore, SURFnet has developed an assessment security selection model that can be used by exam boards to determine which digital testing method is best suited to a particular situation. This model can be found in section 5.4.

## 3.3 Costs

One argument often made in favour of online proctoring (especially by proctoring providers) is the cost saving. The impression is created that online proctoring is almost always less expensive than an exam hall. In practice, the situation is less clear-cut. There are many additional factors at play, which means that the situation can vary from institution to institution and even from study programme to study programme.

In 2013, SURF performed a quick scan of the 'Costs and benefits of digital assessment'[9]. Although this was primarily focused on digital assessment and not on online proctoring, it did produce a number of interesting points that are worth repeating here. Furthermore, it is worth noting that institutions want to use online proctoring not just for existing digital exams, but also for converting existing paper-based exams to digital.

Following the quick scan that took place in 2013, the following points are worth considering:

- The distribution over the different cost centres varies considerably between the institutions. The situation is unique to each institution and there is no uniform answer.
- In 2013, the benefits of digital assessment were primarily qualitative – for instance, that it allows skills to be tested that are difficult to assess on paper.

Reduced costs should therefore not be regarded as a distinct goal for online proctoring or digital assessment in general. It is not the financial savings, but the improvement of assessment quality and educational benefits that should make the business case conclusive.

7. Naturally, there are cases where exam questions are stolen; however exam hall fraud usually involves an individual student copying, passing answers to someone else, or carrying out some other form of individual fraud.
8. See for example: *http://madebyknight.com/knuckle-scanners-cheating-how-to-bypass-proctortrack/*
9. SURF, Quick Scan: 'Costs and benefits of digital assessment'. February 2013; available at *https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/Quickscan+Kosten+en+baten+van+digitaal+toetsen.pdf*

This does not detract from the fact that a financial appraisal must be made before the introduction and use of online proctoring. Some points worth noting:

- Be critical as to whether or not a cost saving is actually achievable. For instance, when exam halls are hired externally, these costs could be saved by using online proctoring. But if an institution is the owner of large exam halls and does not want to or is unable to divest them, the fixed expense (often calculated as a price per square metre) will remain even if it is no longer charged to a particular study programme.
- The prices for online proctoring vary according to both the provider and the method. The more screens a proctor has to follow (one per camera plus the screen capture), the fewer students they will be able to monitor. It may be economically viable to use an exam hall with students taking the exam on their own hardware, while the proctor only monitors the screen capture. The use of your own proctors for the physical monitoring in the exam hall is likely to be more cost-effective (and more secure) than online proctoring in an uncontrollable home situation.

## Costs and benefits for Wageningen University and Research Centre

"We are currently seeing that online proctoring is a little more expensive than our regular exam halls. For regular paper-based exams we use the gym halls, which are normally empty during the day anyway. We only have to move in some chairs and tables, and these are not so expensive. Because we still have standard computer labs for teaching, the same applies to digital exams, i.e. it is cheaper to hold exams on-campus than to use online proctoring."
**Rolf Marteijn, University of Wageningen**

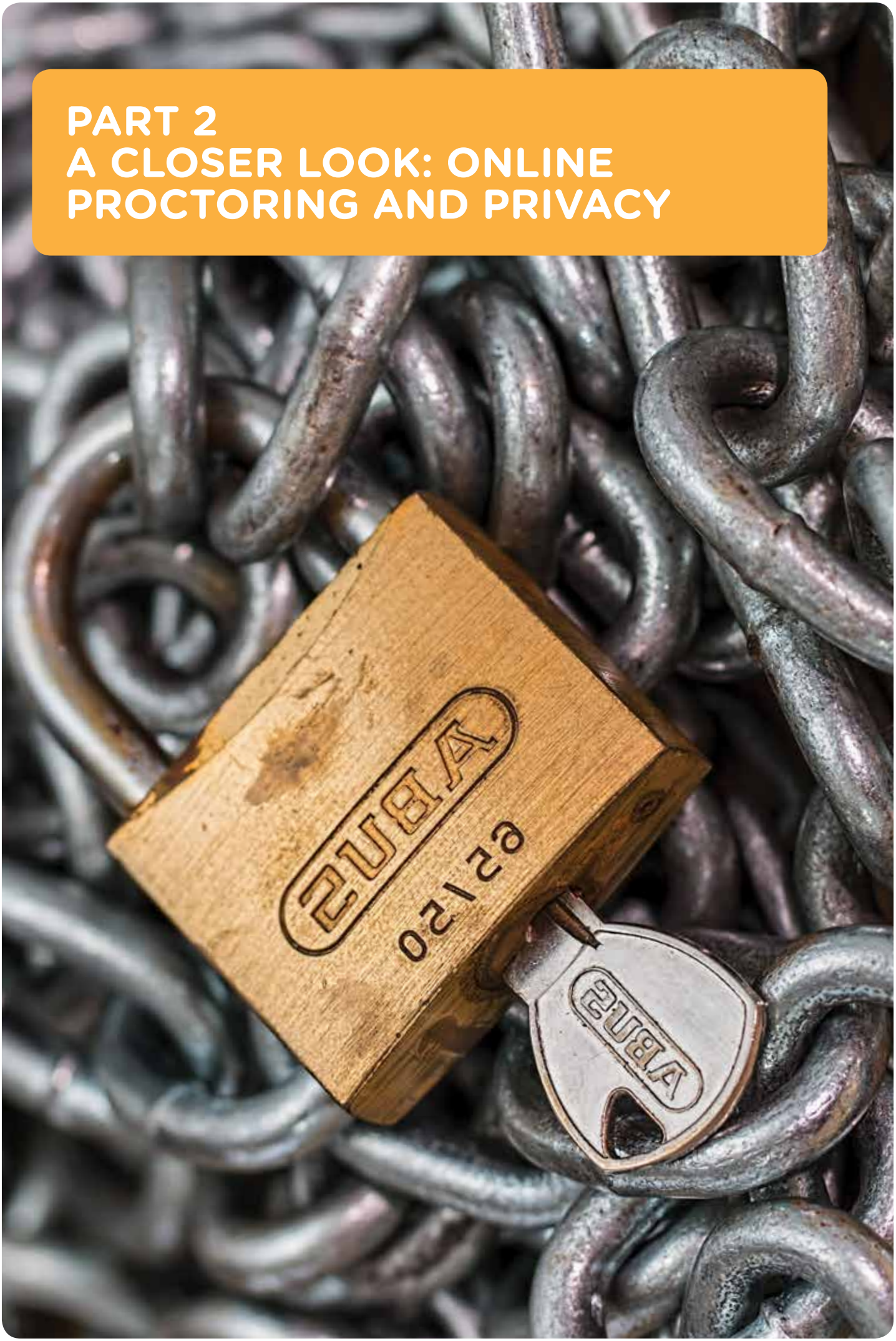
- Sometimes, educational institutions charge students for additional costs involved in teaching and exams[10], and this has also been suggested for online proctoring. However, this is not permitted for normal publicly funded education in the Netherlands. This is because educational institutions may not turn students away and must offer them access to education. This comes part and parcel with an obligation to fund the course through statutory or institutional tuition fees. Asking students to make a financial contribution is only permitted in the case of voluntary optional modules and as long as there is a free alternative, and only in respect of non-publicly-funded education.

### 3.4 False positives

The incorrect detection of potential fraud is a problem for every form of online proctoring. This might be because some providers report every instance of the user looking away from the screen, for example. In 2013 the Chronicle of Higher Education wrote the following about Software Secure: "The company's subcontractor in India, Sameva Global, said it notes 'minor suspicions' in 50 percent of exams; 'intermediate' suspicions in 20 to 30 percent; and 'major' incidents in 2 to 5 percent."[11]
*False positives* occur most often with automated proctoring and least often with live proctoring. In live proctoring, for instance, a proctor can direct the webcam towards the place that the student let their eyes wander to; whereas with recordings it is impossible to be sure whether a student was trying to cheat or whether they just glanced away from the screen. Only a 360-degree webcam would offer a solution for this, but the resolution of these cameras is often low and they would be confusing for the proctor. In short, there is no effective solution for this apart from a live proctor.

10. See for instance *http://www.iso.nl/website/wp-content/uploads/2014/03/Zwartboek-extra-kosten-naast-collegegeld.pdf*
11. Steve Kolowich, 'Behind the Webcam's Watchful Eye, Online Proctoring Takes Hold', 15 April 2013, available at *http://chronicle.com/article/Behind-the-Webcams-Watchful/138505/*

# PART 2
# A CLOSER LOOK: ONLINE PROCTORING AND PRIVACY



# 4. WHAT DOES THE LAW SAY ABOUT PRIVACY?

When an organisation processes personal data, this activity is governed by the Personal Data Protection Act (WBP). What does the WBP mean for online proctoring? There are no standard answers to this question, because an appraisal has to be made in each individual situation.

What is clear is that legal compliance involves more than just having students sign a standard permission form and displaying a privacy statement on the website. The WBP imposes strict requirements on permission requests and information provision, as well as the securing and storage of personal data. The request for permission and the information provided must be tailored to the specific tools used.

This section, which is based in part on SURFnet's 'Guide to Learning Analytics and the Personal Data Protection Act'[12], offers guidance that institutions can use to develop suitable instruments.

## 4.1 What is personal data?

Under the WBP, personal data refers to any data that can be used to identify a person, either directly or indirectly. Names and addresses constitute personal data, as does data about a person's behaviour. Keeping track of what someone is doing during an exam is therefore also a form of collecting personal data. Any data that can be used to identify a person in one way or another constitutes personal data. This therefore refers to more than just names, addresses, camera images or contact details.

Only if it is impossible to make a link between the data and the person – for instance, because random numbers have been assigned and the list linking names and numbers has been destroyed – is the data no longer considered to be personal data in most cases. Even when collection takes place anonymously, the data may still constitute personal data, for instance, when combined with data from another (publicly available) source. Only if it is impossible to draw a link in this way can the data no longer be regard as personal data.

**Aggregation**

If an institution wants to use data from proctoring software for other purposes (e.g. for learning analytics or timetabling), it may be useful to aggregate the personal data in order to draw conclusions on more than one person. The data then loses its status as personal data and, from that moment, the restrictions of the WBP no longer apply. The requirement for this is that the data can in no way be used to identify individuals – not even with the help of other resources and data.

You should also be aware that data may only be used for the purpose for which it was obtained. This means that students must give explicit permission for their personal data to be used for learning analytics or improved timetabling[13].

12. SURFnet, 'Guide to Learning Analytics and the Personal Data Protection Act', November 2015. Available at *https://www.surf.nl/kennisbank/2015/learning-analytics-onder-de-wet-bescherming-persoonsgegevens.html.* Because the WBP largely says the same thing for learning analytics as for online proctoring, this section uses large portions of the text from the guide. It has been adapted to make it appropriate to online proctoring and to ensure correct examples.
13. This is because it the data is still personal data at the moment when it is obtained. The benefit is derived after aggregation because from this point onwards, processing, storage and security are no longer bound by the requirements of the WBP.

**Sensitive personal data**
Sensitive personal data – such as data on an individual's health, political preferences or religion – may not be collected without separate explicit permission, unless there is a legal obligation to do so. In the latter case, the data may only be collected in cases specifically allowed by law. Explicit permission means that a separate request is made for this data, accompanied by a separate explanation of why (and the option to refuse).

Camera images, for instance, almost always contain sensitive personal data, such as data on ethnicity (e.g. on account of the shape of the eyes) or religion (the person is wearing a cross or a kippah). Where camera images are intended to identify people, the data will always be considered sensitive[14]. If a recording is made of an identity document, a legible citizens service number (BSN) also constitutes sensitive data. The requirements for a BSN are even more stringent: it may only be stored if the law explicitly allows it. In the case of online proctoring, this will not be the case and the storage of (camera images of) the BSN is therefore strictly prohibited.

Online proctoring involves the processing of sensitive personal data, and this is expected from the start. Because of this, there are more stringent requirements not only on obtaining permission, but also on careful handling (e.g. storage) of the data.

## 4.2 The statutory basis for personal data processing

Any use of personal data is referred to in the WBP as 'processing'. Processing personal data is only permitted when this is done subject to one of the statutory bases set out in the law. More than one statutory basis may apply; however if no basis can be applied then it is not permitted to process the data – regardless of how convenient, useful, demonstrably effective or desirable that processing might be. Processing is also subject to a number of conditions (statutory bases):

- permission
- performance of an agreement
- legal obligation
- in a life or death situation
- performance of a public function
- necessary to the legitimate interests of the institution

The most relevant statutory bases for online proctoring are 'permission' and 'performance of an agreement'.

**Permission**
The key rule in the WBP is that personal data may only be processed with the permission of the person to whom the data relates. But permission is not obtained at the drop of a hat: you first have to explain exactly what you are going to do and why, and only then can you ask the person if they agree.

Permission must be given freely. This means that the person can freely choose whether to say 'yes' or 'no'. Saying 'no' may not have any significant consequences for the person, such as not being allowed to sit an exam. It is also not permitted to wait to seek permission until after the person has enrolled on on the course – e.g. the first time time they sit an exam. Realistically, a student can no longer refuse permission in that scenario because they are already enrolled on the course.

Permission must be specific. An example of unspecific permission would be: "I grant permission for online proctoring." This is because the term 'online proctoring' is not yet sufficiently established to be used without further clarification. Texts such as "I grant permission for remote proctoring during my exam" are not specific enough either. Who will monitor students, what data is included and what happens to it? A more suitable permission text would be "I grant permission for key logging and the making of video recordings and screen captures from my PC. These images will be stored for a period of ## weeks. The proctor of <company X> and my examiner will receive this data in order to assess whether I have taken the exam in accordance with the rules. Please see our privacy statement for more information." Permission must also be requested separately for the sensitive personal data obtained from the camera images.

14. For more information, see page 25 of the policy rules on camera surveillance of the Dutch Data Protection Authority (Dutch DPA): *https://autoriteitpersoonsgegevens.nl/nl/nieuws/autoriteit-persoonsgegevens-publiceert-beleidsregels-cameratoezicht*

Permission may be granted in advance. You are therefore not necessarily required to seek permission for every exam. Wide-ranging permission could be requested at the start of the year, although the student would then have to receive extensive information. What courses does the permission relate to, how extensive is the monitoring for each course or exam, and what are the consequences for each course or exam? If the proctoring method chosen is the same for all courses, the explanation can of course be relatively simple. However, it will not be possible to make changes to the monitoring during the course of the academic year. Because students have not given permission for this, it will have to be requested once again.

Permission can only be given once adequate information has been provided – i.e. a detailed explanation of what you intend to do. However, it is acceptable to provide a brief explanation (a few sentences) along with a clickable link to a privacy statement that includes further information.

Permission may also be revoked. This does not mean that previous processing suddenly becomes illegal, but no further processing may be undertaken from that point onwards. Just like the original option to refuse permission, it must be possible for the subject to revoke their permission freely. Revoking permission may not carry any significant consequences, such as the person not being allowed to sit an exam. It is permitted to offer the person an alternative (e.g. a written exam), but not to pass on any costs for this.
Revocation of permission can take place at any time without any reason being required, unless the revocation is unreasonable. This is unlikely to be the case, however.

**Performance of an agreement**
The other relevant statutory basis for online proctoring is the 'performance of a contract'. If there is an agreement (contract) between two parties, the contracting parties may process each other's data without having to seek separate permission provided that this is necessary for proper performance of the agreement. However, the processing of the data must be *necessary.* This is a stricter criterion than 'desirable', 'convenient' or even 'most efficient for all concerned'. 'Necessary' implies that there is actually no alternative; i.e. without this personal data, the agreement cannot be fulfilled. This may be thwarted by the fact that online proctoring is very new and can therefore easily be regarded as 'not necessary'. People may take the view that education could also be provided perfectly well without online proctoring. In summary, 'performance of an agreement' does not yet offer sufficient justification for online proctoring.

## 4.3 Securing personal data

Anybody who processes personal data[15] must ensure that the data is adequately secured. This means that all personal data obtained must be reasonably secured against unauthorised access or use. The measures taken must take account of all relevant circumstances, as well as the nature of the data. This applies both to the data that was actually meant to be collected and collateral data – i.e. personal data that was obtained unintentionally.

There is no requirement that security must be absolute. It may be the case that the requirements of the law are met, but personal data is nevertheless misused or misappropriated. This would naturally need to be explained by the institution, and data leaks also usually need to be reported (see below).

There is no generally applicable norm or standard that can offer full compliance with the law in all circumstances. Although certain standards are regarded as adequate in some sectors (such as NEN 7510 in the Dutch care sector), there are none available for the education sector. The 'Legal standards framework for cloud services in higher education'[16] and the 'Standards framework for information security'[17] by SURF and ISO 27001[18] may help you decide whether your security arrangements are adequate.

15. Please note that the term 'process' is used here more broadly that you may think. It refers to any action or set of actions performed on the personal data, including the storage or transmission of data even if no changes are made to the data.
16. Legal standards framework for cloud services in higher education: *https://www.surf.nl/kennis-en-innovatie/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html.*
17. SURFnet Standards framework for information security: *https://www.surf.nl/binaries/content/assets/surf/nl/2015/normenkader-informatie-beveiliging-ho-2015-v1.4.pdf.*
18. *https://nl.wikipedia.org/wiki/ISO/IEC_27001*

**Liability**
Where an institution uses software or services provided by third parties, the institution itself remains responsible and liable for the security of the software or services. This applies even if the supplier has limited their own liability. It makes sense to refuse any limitation of liability or to expand it to allow for cases where harm is caused as a result of a privacy breach.

**Data leaks**
In 1 January 2016, new provisions were added to the WBP in relation to data leaks. As a result, any breach of the security of personal data is considered to be a data leak. As such, the term 'leak' refers not only to the large-scale theft of personal data by external hackers; it also covers unauthorised access to data. This may be students accessing each other's results or a teacher who accesses the personal data of a student without due cause.

Data leaks must be reported. This alerts the data subjects to the problem and allows the regulator to act. The WBP makes provision for two separate reporting obligations:

1. *Reporting to the regulator.*
   A data leak must be reported if it "leads to a considerable chance of seriously detrimental consequences" or if it actually results in these consequences. Reports made to the regulator are confidential.
2. *Reporting to the data subjects*.
   Data subjects (students, employees, etc.) must be informed about any data leak that affects them if this leak would "probably have adverse consequences for their individual privacy".

## 4.4 Access and deletion rights

The WBP also establishes the right of access and the right of deletion.

**Access**
The purpose of an access request is to allow a data subject to find out what an institution knows about them. This means that the entire dossier and all data entries must be provided, and not just what can be accessed using an online tool or provided with minimal effort.
The right of access therefore also applies to camera images and log files. Notes and entries made in offline dossiers are normally also covered by the right of access.
A request for access to personal data must always be honoured. There is no possibility to refuse access for reasons of 'corporate secrecy' or to protect the copyright of the tool supplier. The purpose of the access is also irrelevant, and a request may therefore not be refused simply because it is unclear what the requester intends to do with the information.

With online proctoring, it can be difficult to be fully comply with this obligation if the necessary functionality has not been built in. The maximum charge for each access request is 5 euros[19]. Requests may be refused if an excessive number of requests are made in a short space of time.

It could be expected that students would wish to access their exam data in the context of an appeal or objection procedure, for example. In order to honour these requests, it is important to establish an adequate process or to have the supplier to build one into the software.

**Deletion**
Data may not be stored for any longer than necessary for the purposes for which it was collected. For online proctoring, this specifically means that data must be deleted once the assessment of the exam has been confirmed and an appeal or objection is no longer possible. Furthermore, a person may ask for their personal data to be deleted. This request must be honoured unless there are compelling reasons not to do so. If aggregated combinations have been made using personal data, these combinations do not have to be erased following a deletion request because these combinations do not contain any personal data.
If the data is contained in source files for scientific research, these may be kept, but only in order to verify the research (and hence not for other research, not even if it follows on from the research in question).

19. In accordance with the Decree on fees for WBP data subjects ('Besluit kostenvergoeding rechten betrokkene Wbp'), available at *http://wetten.overheid.nl/BWBR0012565/geldigheidsdatum_24-12-2015.*

If deletion is not technically possible (because back-ups are stored externally, for example), the data subject at least has the right to ensure the data is segregated so that it can no longer be used for other purposes. The relevant parts of these back-ups should therefore no longer be available for unrestricted use by the institution. Otherwise, the deleted data would simply reappear if the back-up were restored.

## 4.5 Automated decision-making

The WBP prohibits fully automated decision-making or the imposition of sanctions based on a personality profile. A profile of this kind is understood to comprise a set of personal data that creates “an image of certain aspects of a person’s personality”. This could relate to someone’s creditworthiness, reliability or their behaviour.

**Decision-making and online proctoring**

Fully automated decision-making is regarded by some as the future of online proctoring, but it is prohibited by the WBP. It is therefore not permitted to allow the software to declare an exam invalid. This decision must always be taken by a human (a lecturer), who must make their own assessment in order to do so. An exam may thus not be declared invalid “because the system has identified too many abnormalities”.

**Profile information**

The prohibition on automatic decision-making relates only to profile information. That means it is permitted to fail a student entirely automatically based on the number of errors they make, but it is not permitted to exclude someone as a fraudster when they suddenly score a 9.5 despite a history of failing exams. The same applies if the software establishes that a student’s keystrokes show that someone else other than the student was typing. In itself, this may not be used as a basis for concluding that fraud has been committed.

**Objections**

If a decision or measure has a “considerable impact” on someone and is based on their personality profile, it should always be open to objection. In practice, it is defensible for this option to be offered after the measure has been imposed, provided that there is still time to correct the negative consequences. This can be implemented by adding (for example) “Do you disagree? If so, please contact the exam board within 4 weeks” when informing the student that they have to take another course.

## 4.6 Third-party services

Online proctoring will often involve the use of third-party services. This could be when software is purchased and implemented by the institution; however the provision of the service itself (such as data storage or the deployment and training of human proctors) is also increasingly outsourced to third parties.

**Points to consider**

When using third-party software or services, there are two important points to consider:

1. The institution itself is always responsible for the quality of the service and for any problems vis-à-vis the student. This will also be the case when the software supplier does not wish to accept any liability. The student cannot release the institution from this liability through a limitation of liability in the acceptance statement or a disclaimer in the software’s splash screen (for example).
2. If the service provider also obtains personal data, as is the case with cloud services, then the institution must agree separate arrangements regarding what the service provider may do with it. The service provider then becomes a processor under the WBP.

The arrangements referred to in the second point must be set out in a processing agreement.

## 4.7 Processing in other countries

The WBP is based on European rules, which are the strictest in the world. Europe is at the forefront when it comes to personal data protection. The European rules state that personal data may only be stored or processed in countries that have an 'adequate' level of protection. This means that the country must have rules as strict as Europe itself. The purpose of this is to force other countries to adopt personal data protection legislation.

A further elaboration of this can be found in the 'Legal standards framework for cloud services in higher education'[20]. This document sets out the standards governing confidentiality, personal data protection, ownership and availability for cloud service providers in the higher education sector in the Netherlands.

**Outside Europe**

There is no obligation to store personal data in the Netherlands. Every country within the European Economic Area (EEA) is essentially adequate. The situation is more difficult with countries outside the EEA because there are very few countries that meet European requirements. The United States is not compliant, as was confirmed in a recent ruling by the European Court of Justice. At the time of writing, the use of American suppliers is therefore problematic. The most up-to-date information can be found on the SURF website.

**European subsidiary**

A special situation arises when personal data is stored in a European country in a data centre that is managed by a US company or the subsidiary of a US company. Although that party is subject to European law, it also appears that the US government considers itself competent to request the release of personal data from that data centre under the US Patriot Act or other US legislation. At the time of writing (late 2015), a law suit on this issue against Microsoft is ongoing. If it is found on appeal that the US justice authorities have the right to request data from European data centres owned by subsidiaries of US companies, it will be impossible to use these data centres for the storage of personal data.

## 4.8 Law enforcement

Enforcement of the WBP in the Netherlands has always been a little neglected. The reason for this is primarily the limited authority of the Dutch Data Protection Authority (DPA) to impose fines. An amendment to the law on 1 January 2016 has changed this, and a fine can now be imposed for the breach of almost every obligation contained in the WBP. This also applies to any failure to ensure an adequate level of security, and to any failure to report something when there is an obligation to do so. In theory, the fine can be up to 810,000 euros, the highest category in administrative law. The regulator will first have to publish policy on which types of fines will be imposed for which types of breach.

Breaches can only be fined after a binding instruction has been given and this has not been acted on. A binding instruction is an enforcement action (under article 5:2 of the General Administrative Law Act) that is imposed following a breach. It might specify how security must be improved, for example. If the breach was deliberate or was the result of "seriously culpable negligence" then the regulator may impose a fine immediately. It is not yet clear in which circumstances this would be the case. If an organisation does not have a policy for identifying and reporting data leaks, it will be easy to conclude that there has been seriously culpable negligence.

20. *https://www.surf.nl/kennis-en-innovatie/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html*

### 4.9 Specific recommendations

Based on the privacy aspects described in this section, a number of online proctoring recommendations have been prepared for institutions:

1. Draft a separate privacy statement for online proctoring and state the purpose in it. Make clear what data will be collected and what will happen to that data.
2. The privacy statement should also specify that data will be destroyed as soon as the exam results have been finalised. Ensure that both the institution and the supplier strictly adhere to these retention limits.
3. Request permission:
   a. at a moment when the student can still refuse without suffering any consequences;
   b. after providing clear information;
   c. and offer an option to proceed normally if permission is refused (i.e. do not refuse a student for the exam, but provide an alternative).
4. Formulate permission requests explicitly as yes/no questions, and ensure that the question itself makes clear what permission is being asked for.
5. Agree with the supplier that they should provide detailed information, even for tool updates, so that this can be included in the privacy statement.
6. Supervise the use of the data and ensure that the only people who have access to it are the people who require it for the performance of their duties (for instance, the examiner and the exam board).
7. Make an option available to download online proctoring data (access request) and, where appropriate, to correct it (in the case of obvious errors).
8. Find out which tools make automated decisions that have a considerable impact on students. Design the process so that the ultimate decision is made by a human, and always offer a clear opportunity to raise an objection.
9. Conclude data processing agreements with the suppliers of online proctoring tools. In these agreements, stipulate:
   a. that they are liable for data leaks;
   b. that they may not use the data for their own purposes;
   c. that they must provide detailed information to students about how the tools work.
10. Prepare a policy to prevent data leaks and security breaches.
11. Respond positively to personal data protection concerns and objections from students, and provide alternatives that will allay these concerns.

# PART 3
# A CLOSER LOOK:
# ANTI-FRAUD MEASURES

# 5. HOW RELIABLE IS ONLINE PROCTORING?

This section describes the various solutions that online proctoring software offers to prevent fraud. It also looks at the ways in which students may try to commit fraud. Based on this and together with the assessment security selection model in section 5.4, an exam board can assess whether online proctoring is suitable for a particular part of the curriculum.

Security and fraud prevention attract a great deal of public interest, but at the same time they are difficult subjects. The higher the security requirements of an examination, the more expensive and more impractical it will often become, and the greater the impact will be on the privacy of students. Even exams held in regular exam halls are not 100% secure, but educational institutions and exam board are very experienced with this environment so they are able to properly assess the risks and restrict them to an acceptable level.

## 5.1 Preventing fraud

Online proctoring offers various means to increase security and prevent fraud.

**Cameras and microphones**

With almost all proctoring software, the proctor can watch over the exam via the student's webcam. There are also variants that use two webcams. The second webcam is often provided by a phone or tablet that must be placed behind the student. This ensures that a larger part of the space is visible and gives the proctor a view of the student's screen and keyboard.

**Screen capture**

Another method that almost all suppliers use is screen sharing, which allows the proctor to view the student's screen. The proctor can then see what programs are open and whether the student is using prohibited sources.

**Lock-down browser**

The lock-down browser is a feature that is not only used for online proctoring, but also in other forms of digital assessment. Only the assessment environment and specific, authorised applications can be used. The options can vary from one supplier to the next. It is important that this feature is not overestimated. The fact that someone cannot launch other applications does not mean that they cannot run in the background, and most lock-down browsers can be bypassed (on the user's own device) with sufficient IT knowledge. This does not make it completely useless, but for online proctoring it should be seen as complementary to screen capture and camera images.

**PC logging**

Some proctoring suppliers allow you to see in detail what happens on the student's computer. The extent differs from one supplier to the next, but the potential is enormous. Active processes[21] can be scanned and the memory can be read, for example. To achieve this, the software must have full access to the PC. This makes it a very powerful resource that would have a far-reaching impact on privacy.

21. These might be applications that remain open, even if only in the background.

**Keystroke dynamics**
A user can be identified not just by what they type (a password), but also by the way they type it[22]. Keystroke dynamics cannot yet be used to positively identify a person with certainty, but they are increasingly good at ruling someone out. If the keystroke dynamics of a student are known, the software can issue an alert that the person sitting the exam is probably not the student who should be sitting the exam. This could prompt a thorough review of the camera images. It is important to understand that keystroke dynamics represent sensitive personal data, comparable to a fingerprint[23].

## 5.2 Online proctoring risk factors

A student can attempt to commit fraud in a variety of ways. The list below is not exhaustive, but gives a good indication of the possibilities. For each fraud method, we indicate whether it can be combated by online proctoring and, if so, how.

**Hardware and software**
With online proctoring, the student uses their own PC or laptop[24]. This means that there are various ways to commit fraud during an exam.

- *An extra browser or tab*
  Perhaps the most common method of committing fraud is when the student tries to look up the answers to questions during an exam using the internet.
  ⦸ *Countermeasure:* This method is easy to combat. Screen captures and an extra webcam ensure that the student will be caught. A good lock-down browser is also often sufficient.

- *A second person monitoring or controlling the PC*
  Just as an online proctor can monitor the PC, a student can give someone else remote access to their PC. This other person can then see their screen and even control the keyboard and mouse, which means they could complete the exam while the student is still sitting at their PC.
  ⦸ *Countermeasure 1:* If the proctor can see the student's keyboard and mouse then this would be detectable, the movements would not match what is happening on the screen. However, the chance that a proctor would see this is small[25].
  ⦸ *Countermeasure 2:* Only good logging software could combat this. This software can see in detail what software processes are running on a PC and what external connections are being made.
  ⦸ *Countermeasure 3:* In cases where the exam requires longer answers, keystroke dynamics are a good solution for recognising who is writing the text.

- *Software that provides answers*
  A student could install software that scans the questions on the screen and looks up the answers. It could show these on the screen, or possibly even fill them in directly.
  ⦸ *Countermeasure 1:* If the answer is clearly displayed on the screen, this would be easily detected using screen captures.
  ⦸ *Countermeasure 2:* It is more difficult to detect if the software directly inputs the answer. In that case, only good logging software would offer a suitable solution.

- *A virtual machine*
  A virtual machine is a simulation of an extra PC hosted within the usual computing environment. If the exam is taken within the virtual machine, the proctoring software will only see that PC's screen, and the software running on the host PC would be invisible. This makes many of the previously mentioned and resolved fraud options possible again. An additional problem is that there are good reasons why a student might use a virtual machine. If the exam or proctoring software only runs on iOS (Apple) and Windows but the student normally uses Linux, for instance, then they would have to use a virtual machine.
  ⦸ *Countermeasure 1:* Assuming that the use of a virtual machine during the exam is prohibited, it is possible to detect this using advanced software. However, it is not possible on all hardware and with all virtualisation software.

22. Jiexun L., Rong Z. and Hsinchun C. (2006). 'From fingerprint to writeprint'. Communications of the ACM, Volume 49 Issue 4. Available at *http://www.disciplineoforganizing.org/wp-content/uploads/2013/01/FingerprintToWriteprint.pdf.*
23. This might include the speed at which the person types, the letters that slow them down and how long they hold down keys for. For more background information, see: *https://en.wikipedia.org/wiki/Keystroke_dynamics.*
24. If proctoring software is used within the institution's own exam hall and on the institution's own computers, this section will of course not apply.
25. It is possible to disable the local keyboard so that the student can type without anything happening on the screen. If they type approximately in sync with the person completing the answers for them, then this would be difficult to detect.

⦸ *Countermeasure 2:* A second camera positioned behind the student would also help, because the screen would be fully in view. This would prevent part of the fraud, such as having extra windows open. However, this would not detect any software running entirely in the background.

**Help in the environment**

• *Another person in the room*

If there is another person in the room, the person sitting the exam could consult with them (either verbally or using gestures).

⦸ *Countermeasure 1:* A microphone would be partly able to detect this if the two people were speaking to each other. This would make it relatively complicated for the student and the other person to communicate.

⦸ *Countermeasure 2:* The use of cameras would help here, of course. The student often has to show the entire room to the camera before the exam starts. But a second person could hide outside the field of view, especially when only one camera is used. They could then give instructions using gestures or notes[26]. In brief, certain measures could make this method of fraud more difficult, but it cannot be excluded entirely.

• *Someone else using the PC*

Just as in a regular exam setting, attempts are sometimes made to have someone else sit the exam.

⦸ *Countermeasure:* Ask someone to confirm their identity by showing their student card or identity document to the webcam. Important: if an identity document is requested, the citizen service number (BSN) may not be visible.

• *Hidden crib sheets*

Crib sheets are regularly used in normal exam halls, and this is likely to increase rather than decrease when students take exams at home.

⦸ *Countermeasure:* The use of crib sheets cannot be eliminated entirely. Camera images can help combat this, especially if a good and thorough check of the entire room is made before the exam. The room will never be fully visible during the exam, and hidden crib sheets remain a possibility.[27]

• *Remote monitoring by a third party*

We already discussed the possibility of detecting someone using software to monitor the PC remotely. However there are other ways to monitor exams, such as by placing a separate camera (in a phone or tablet) behind the student. It is also possible to split or intercept the video output signal[28].

⊗ *No countermeasure possible:* When executed well, this method cannot be detected (a small camera is easy to hide between a row of books). The challenge for the student is to ensure that the other person can send them the answers. What was true of crib sheets is also true here: this activity can always be hidden effectively because the entire space is never fully in view. The longer and more extensive the answers, the more difficult this type of fraud becomes. This method is particularly easy to execute for multiple-choice exams because only a small amount of information needs to be communicated (the number of the answer)[29].

## 5.3 So what does this mean?

With a little creativity, the list of opportunities to commit fraud under online proctoring is almost endless[30]. Based on the examples given in this section, we can draw a number of conclusions.

- Fraud involving manipulation of the hardware or software can usually be detected. However, this often has far-reaching implications for the student privacy.
- If the education institution does not have any control over the space where an exam is held, there are many ways to commit fraud that are (almost) impossible to detect. For this reason, online proctoring can never be as secure as holding exams in an exam hall.

26. This would be easiest to do if the second person could see the screen, but even if this were not possible then the student could talk out loud every now and again. It is difficult to ban talking altogether because some people like to think out loud.
27. It is easy to imagine plenty of ways to conceal a crib sheet during a room inspection, only to make it visible again during the exam. For instance, it could be covered up with something that can be removed using a thin piece of string. This is almost impossible to detect as long as the crib sheet's location remains out of shot during the exam.
28. This can be done using a small box positioned between the PC and the monitor that cannot be detected by the PC. The signal can then be sent to another person either via a cable or wirelessly.
29. Example: the student could hide four small lights in their room that are controlled by the person helping them. Each light would stand for an answer, either A, B, C or D. There are dozens of surreptitious communication methods that are difficult or impossible to detect.
30. See for example: *http://madebyknight.com/knuckle-scanners-cheating-how-to-bypass-proctortrack/*

Despite this, online proctoring is certainly useful as a resource that can be used to facilitate the organisation of digital exams in certain situations. However, it is important to make a well-founded decision that weighs both the importance and the risk of the specific exam, as well as the benefits.

To help exam boards or assessment boards reach a decision for each situation, SURFnet has developed an assessment security selection model. This is described in the next section.

## 5.4 Assessment security selection model

When deciding on a suitable method for digital assessment, we currently look primarily at what is at stake with a specific exam. Often we only distinguish between two levels: high-stakes exams and low-stakes exams. This results in a lot of nuance being missed:

1) All summative exams are regarded as high-stakes exams, including both interim tests and final exams.
2) No distinction is made based on the assessment format (multiple choice, oral exam or essay) despite the fact that this has a major impact on the suitability of different assessment methods[31].

To enable a more nuanced decision, SURFnet has developed a model in which both the risk of fraud and the importance of the exam result are taken into account. This model is not only suited to online proctoring, but can be used more broadly: it can support exam boards in determining whether the intended assessment situation is adequate, or to see what assessment methods would be suitable within the curriculum.

### 5.4.1 The importance of the exam

The selection model identifies four levels to indicate the importance of an exam:

- *Low*
  These are formative exams or online courses with no recognised social value. This might include MOOCs such as courses by Coursera, programmes offered by the Khan Academy or open courseware.
- *Medium*
  At this level, the exams do not directly contribute (significantly) to the transcript, but there are still consequences attached to them. Examples include small weekly interim tests that together might result in a extra point, or tests that give access to a module, an exam or an internship.
- *High*
  These are exams that have a direct and significant impact on the student's study credits. This will apply to all exams for modules that attract study credits, but also for partial examinations that together contribute towards the final assessment.
- *Very high*
  This category includes specific modules or tests which demand higher standards of fraud prevention[32] due to the nature of the courses or certain (legal) consequences. For instance, exams which allow access to professional practice as a lawyer or in the judicial system (civil effect), or to obtain BIG registration[33]. It may also include exams which seen as particularly important for other societal reasons, such as the CITO exam, secondary school leaving exams or language and maths tests in teacher training colleges. Graduation assignments also come under this category, as they determine whether or not the student is awarded a diploma.

### 5.4.2 The risk of fraud

The selection model identifies three levels to indicate the risk of fraud in relation to a particular exam:

- *Low*
  This is an exam where the student submits an entirely unique work, such as a thesis, essay, practical assignment or an oral exam. In these cases, fraud prevention focuses on detecting plagiarism and establishing that the student has done the work themselves.

31. This is because the risk of fraud is much greater with multiple choice tests than in an oral exam.
32. These may be requirements imposed by the exam board, but may also ensue from the general wishes of society at large or from legislation and regulations. The ultimate assessment, however, will always be made by the exam board.
33. The register of professionals working in the healthcare sector. Only registered persons are authorised to practise their professions. See also: *https://nl.wikipedia.org/wiki/BIG-register*

• *Medium*
An exam requiring unique answers, but which is not entirely the student's own work (as with a thesis or essay). This may be a written test with open-ended questions, where the answers are of sufficient length to be unique to each student. This might be a test requiring advanced mathematical calculations on paper, or where answers have to be substantiated with extensive text.
• *High*
Exams in which only a single answer is possible, and in which students in most cases do not give unique answers. This includes all closed-ended questions, including multiple choice.

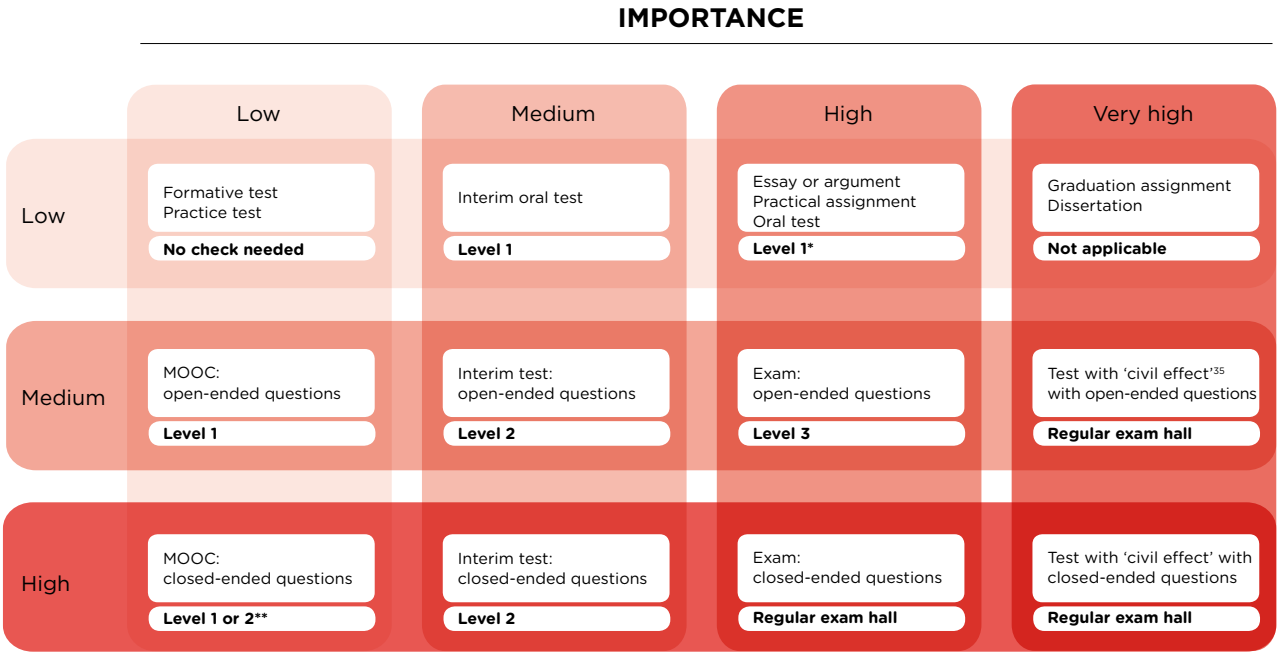
**5.4.3 The selection model**

The selection model is based on the allocation of risk and importance, as described above. The model below has been partially completed to illustrate how it can be used. Every exam board or assessment board can adapt it to their own context. When doing so, they should also take into account the context of the curriculum. For example, if certain knowledge is assessed multiple times during a study programme, the exam board may attach less importance to an earlier test than to a later test. After all, the knowledge would be retested and a student committing fraud would then find themselves caught out.

For each combination of importance and risk, the model indicates the corresponding security level. This may mean, for instance, that a selection is made between different forms of online proctoring, or that a decision is made between BYOD and a fixed configuration for digital assessment.

In online proctoring, three levels have been identified:
• *level 1:* screen capture and a single camera;
• *level 2:* screen capture and two cameras;
• *level 3:* full logging, screen capture, two cameras and only live proctoring or a recording.

The security offered by online proctoring is currently inadequate for some forms of education that are both high risk and high or very high stakes. A different assessment could be considered in order to reduce the risk of fraud. That might be a well-equipped computer lab, or possibly a secure form of BYOD exam within the institution's own exam hall. The regular exam hall[34] with paper-based exams is also always a good fall-back option.




* Naturally, online proctoring is unsuitable for essays and work performed over long periods of time. It is particularly suited to oral exams, for example.
** For MOOCs, this depends on the value placed on the MOOC.

34. No study was made of the possibilities and security of BYOD solutions or existing computer labs for the purposes of this white paper. However, in these situations the institution does have control over the environment (the weak point in online proctoring), so they can probably be made more secure than would ever be possible with online proctoring.
35. For instance, authorisation to enter professional practice as a lawyer or in the judicial system.

# CREDITS

**Author**
Lex Sietses (SURFnet)

**Contributions by**
Willem Brouwer (Amsterdam University of Applied Sciences)
Natasa Brouwer-Zupancic (University of Amsterdam)
Michiel van Geloven (SURFnet)
Evelijn Jeunink (SURFnet)
Meta Keijzer-de Ruijter (TU Delft)
Rolf Marteijn (Wageningen University)
Alf Moens (SURFnet)
Annette Peet (SURFnet)
Guusje Smit (University of Amsterdam)
Simon Theeuwen (Interstedelijk Studenten Overleg)
Sebas Veeke (SURFnet)
Josephine Verstappen (LSVb National Student Union)
Marja Verstelle (Leiden University)
Jenny de Werk (SURFnet)
Stefan Wirken (LSVb National Student Union)

**Editing**
Daphne Riksen - Ediction

**Design**
De Hondsdagen, Bunnik

**Photography**
Lars van Rooijen Photography
Yuri Samoilov www.flickr.com/photos/yusamoilov/13334048894
Steve Buissinne https://pixabay.com/nl/users/stevepb-282134/

SURFnet
admin@surfnet.nl
www.surf.nl/surfnet


March 2016

SURFnet
Hoog Overborch Offices (Hoog Catharijne)
Moreelsepark 48

PO box 19035
3501 DA Utrecht, The Netherlands

+31 (0)30 887 873 000

admin@surfnet.nl
www.surf.nl/surfnet