

Unlocking seamless access: the case of Feide single sign-on in Norway

CASE STUDY – NORWAY

Authors: Greta Björk Gudmundsdottir, Ola Erstad & Øystein Gilje, University of Oslo

30 June 2025

Contents

Summary.....	3
Introduction.....	3
Method.....	4
Participants.....	5
Data collection	6
Analytical procedure	6
Feide background and context.....	7
Data in use for teaching and learning	11
Parental access.....	11
Rights, regulations and privacy	13
Data quality.....	13
Equal access – digital divides	15
Parental Consent.....	16
Data governance	17
Guidance and Support.....	18
Expert panel	19
Commercial actors	19
Conclusion and key implications	20
Equity and inclusion considerations	22
References	23

Summary

This case study introduces the single sign-on service (SSO) in Norway called *Feide*. SSO is an authentication method streamlining access to multiple digital resources, apps and cloud services. *Feide* stands for “joint electronic identity” and is a national service in Norway run by the Norwegian Agency for Shared Services in Education and Research (Sikt). The case study explores how this service has developed and its role and impact within the Norwegian education system. In addition, a pilot project intending to involve parents in this service will be introduced. We have interviewed key stakeholders on national and municipality levels about *Feide*. The key takeaways and implications are that such a national service provides security and trust for all users and content providers in handling of data.

Introduction

In the education sector, institutions establish unique communication and security protocols based on their network infrastructure. This infrastructure supports various systems and applications within a network, including wireless access, servers, access controls, certificates, and internal and external devices, facilitating communication among different sub-systems. In this report we will introduce the case of single sign-on service (SSO) in Norway called *Feide*. SSO is an authentication method streamlining access to multiple apps and cloud services and *Feide* which stands for “joint electronic identity” is a national service in Norway run by the Norwegian Agency for Shared Services in Education and Research (Hereafter Sikt).

Sikt delivers products and services for the education sector, both in terms of common infrastructure and support of digitalisation, data sharing and open research together with *Feide*. *Feide* which is a national solution for secure sign-on and data sharing, applies to the whole education sector; thus both primary and secondary education as well as tertiary education and research are users of *Feide*. With *Feide*, students, educators and researchers get a safe and accurate access to a variety of digital services by using the same username and password. In addition, *Feide* offers two-step authentication where greater login security is required.

Overall, a national SSO service like *Feide* brings numerous benefits and has been widely embraced in the education and research sector in Norway as it improves both security, reduces costs, and increases efficiency. It is essential to *simplify access* to different digital services for the users. Other benefits are that it eliminates the need for users (in this case students, teachers, and researchers) to remember individual and multiple usernames and passwords for different services, which can be a daunting task. SSO can be argued to save time and reduce frustrations for users, while *improving security* and reducing the risk of unauthorized access through weak or shared passwords is essential. *Feide* therefore enables secure and seamless data sharing while also protecting its users’ privacy. SSO services can also be seen as increasing productivity and saving time as the

app/service in question is easily accessible and the work can start immediately. The burden on school administration is evident and can be reduced considerably by using SSO.

In Norway there are 357 municipalities and 15 counties which are the so-called *school owners* and in charge of providing education for its inhabitants. The municipalities are in charge of providing primary and lower secondary education whereas the counties are in charge of providing upper secondary education. The support for data sharing in *Feide* makes it easier for school owners to keep track of which services receive information on their users. In that way, *Feide* ensures *control* over data sharing which also provides service providers and producers of teaching materials and learning resources the information needed to offer teaching materials and other digital services adapted to the needs of the users.

Furthermore, *Feide* has functionalities to enable parental access, but schools must define and enable the scope of access and give parents the opportunity to engage actively in their children's education. Parental access is considered essential as it provides parents with insight into their children's schoolwork and learning, which has become more challenging due to digitalisation. Therefore, in the following case study our point of departure is the research question: *What is the role and impact of a national single sign-on service (SSO), such as Feide in Norway, on the provision of digital services for education and the involvement of different stakeholders such as parents?*

Furthermore, we will structure this case study as follows. After this introduction we introduce our methodological approach including how data collection was conducted, the sample of participants and how the empirical data was analyzed. We then turn to our interviews and present *Feide* through the experiences of our informants starting by briefly discussing the history and background of *Feide* in the Norwegian education sector. We then introduce recent developments of parental access called the *parental-pilot*. This involves new possibilities and challenges emerging when planning for opening up for a new group of users. Finally, we draw conclusion and recommend future actions.

Method

As explained earlier *Feide* is a national initiative, aimed at facilitating secure access to digital learning resources for educational institutions across Norway. This section presents the methodology employed for the collection of data for this *Feide* case study. The primary data source consists of semi-structured interviews conducted with key stakeholders involved in the *Feide* initiative. These stakeholders include representatives from the Norwegian Agency for Shared Services in Education and Research (Sikt), The Norwegian Directorate for Education and Training (hereafter UDIR), and various municipality representatives involved in the parental pilot of *Feide*.

Participants

The selection of interview participants was based on their expertise and involvement in the *Feide* project. The informants comprise individuals from diverse organisations and municipalities, bringing a range of perspectives on the implementation and impact of *Feide*. Through their insights, this case study aims to gain a comprehensive understanding of the challenges, successes, and opportunities associated with the national implementation of *Feide* in general and the parental-pilot in particular. Table I provides a list of the participants and their organisation.

Table I. List of participants (pseudonyms) and organisations

Pseudonym	Organisation
Heidi	SIKT
Samuel	SIKT
Roger	UDIR
Karen	UDIR
Richard	Municipality a
Benjamin	Municipality b
Kurt	Municipality c

One interesting aspect is that the majority of these informants have teacher background, but have now moved into more advisory and strategic positions within their respective municipalities. This means that they have a genuine understanding of the educational practices in schools and how technologies might be implemented and used for the enhancement of teaching and learning.

According to the ethical guidelines of the project, written and oral consent were obtained from all the participants prior to the interviews taking place. The consent process included an explanation of the case study's objectives and the purpose of their involvement. Participants were provided with clear instructions about their right to withdraw from the study at any point without any negative consequences. Emphasising confidentiality, privacy, and data protection, the participants were assured that their responses and personal information are handled with the discretion and in compliance with GDPR. The informants in this case study were guaranteed participant anonymity. To uphold the anonymity of the contributors, pseudonyms were assigned to maintain confidentiality and prevent identification of individuals in this report. Only the research group in Norway has access to the transcribed data and knows the identity of the participants.

Data collection

Interviews were carried out via Zoom between January and February 2024. The participant received the semi-structured interview guide some days in advance and could therefore prepare for the interview session. The interviews lasted from 45-60 minutes each. A follow up interview was conducted in early January 2025 to include recent developments within the Feide project.

The University of Oslo automatic transcription tool *uio.autotekst* was utilized to transcribe the interviews. The researcher responsible for conducting each interview carefully reviewed each transcription and made necessary corrections of apparent errors in the auto-translation. In case of ambiguity, the respective audio files were played, and the transcripts revised accordingly if needed. The final versions of the transcripts were then shared with the informants for their approval. Additionally, they were offered the opportunity to adjust any segments of the transcript to ensure accuracy and alignment with their perspectives. Only the transcribed sequences used in this report were then translated to English.

Analytical procedure

This case study is analysed based on the analytical framework developed by the [Agile EDU literature review on datafication in and of education](#) (Erstad et al., 2024). The analytical framework views data use and datafication as an ecosystem of various education stakeholders, each with their own priorities and perspective on tackling the challenges of education using data. This ecosystem is based on the interrelationship between three pillars: (1) data in use for teaching/learning; (2) regulations, rights and privacy and (3) data governance. At the core of these three pillars is the digital data generated by students and teachers (see further Erstad et al. 2024).

The findings are represented under the three subsections, each focusing on one of the pillars of the Agile EDU analytical framework. We started by listing the questions from the semi-structured interview guide under each of the subsections. Upon consolidating the semi-structured interview guide, the authors conducted a thorough examination of the data, which involved careful consideration of questions that could potentially overlap the subsections. The goal was to ensure that each question was appropriately placed within the sub-sections to accurately capture the multifaceted responses provided by the informants.

Following this initial preparatory stage, the transcribed interviews were reviewed by the authors. The focus was on identifying key insights, and patterns in the informants' responses. Through a systematic coding process, the authors stratified the data according to the predefined questions from the semi-structured questionnaire, allowing for a comprehensive analysis of the transcribed interviews. Moreover, the iterative nature of the coding process facilitated comprehensive data exploration, revealing insights underpinning the findings presented in this report.

Feide background and context

In this section we provide a short historical background and some contextual information on *Feide*.

SSO is a method that allows users to register themselves only once to log on any service provider, without the necessity to create new accounts with new usernames and passwords for each of them (Pashalidis & Mitchel, 2003). In the education sector, school and university students use a variety of learning management systems, applications, and cloud services. Many of these provide various solutions for SSO. In Norway the most widely used is *Feide* which has offered SSO services since the year 2000. Originally it was developed for universities and the higher education sector. One of our informants, Roger, tells us about the history of *Feide* starting with a focus on student administration systems using *Feide* in the early 2000s, initially in connection with secure login. Back then, *Feide* began to emerge as a secure authentication method. When the use of digital learning resources became more common in primary and secondary education, the need for *Feide* increased dramatically.

Feide is commonly employed and recognised as the safe service provider within the education system in Norway. In response to the various services and applications with disparate passwords, *Feide* was initiated to address the challenge faced by students and teachers in managing their credentials. With the aim of consolidating and streamlining the digital ecosystem, *Feide* seeks to establish a unified connection between the individuals and the range of services they access.

Historically *Feide* became a part of The Norwegian Centre for ICT in Education when it was established in 2010. It was formed through the merger of various organisations, including utdanning.no, ITU, and UNINETT ABC. The Centre was a governmental agency under the Ministry of Education and Research, and its purpose was to enhance the quality of education by integrating ICT into schools, leading to improved learning outcomes. The primary target groups for the Centre were kindergartens, primary and secondary education, as well as preschool and teacher education programmes. The Norwegian Centre for ICT in Education took over tasks from UNINETT ABC, which had been involved in the development of *Feide*. The Centre was responsible for facilitating the implementation and use of *Feide* in Norwegian schools. On January 1, 2018, *Feide* became a part of UDIR - the Directorate for Education and Training when the Norwegian Centre for ICT in Education merged with the UDIR. Today, *Feide* is administered by Sikt (www.Sikt.no). Sikt collaborates with UDIR (www.udir.no) which is the executive agency for the Ministry of Education and Research.

From the start *Feide* has been financed by its users. Roger explains how the “host organisations”, for example a primary or secondary school, pay for the use of *Feide* based on the number of students, while the service providers (for example publishing houses) do not pay any connection fee to *Feide*. Still, they need to cover their own costs associated with integrating *Feide* with their products. Financial commitments between the service provider and the host organisation are regulated in an agreement between these parties. For the service providers, *Feide* represents a

significant potential with over 1.5 million users. UDIR formally funds and caters for new services such as the *Feide* parental pilot (see further section 4.1).

When asking our informants to describe what *Feide* is and what role it plays in Norway one of our informants, Heidi, explains it as “the hub where digital services and all the schools in the country as well as many universities and colleges are connected”. At present *Feide* connects 1.5 million users with around 2000 (including higher education) different digital services (see Figure 1 for numbers concerning primary and secondary education) which makes *Feide* a central hub or an ecosystem for various services and users within the education system.

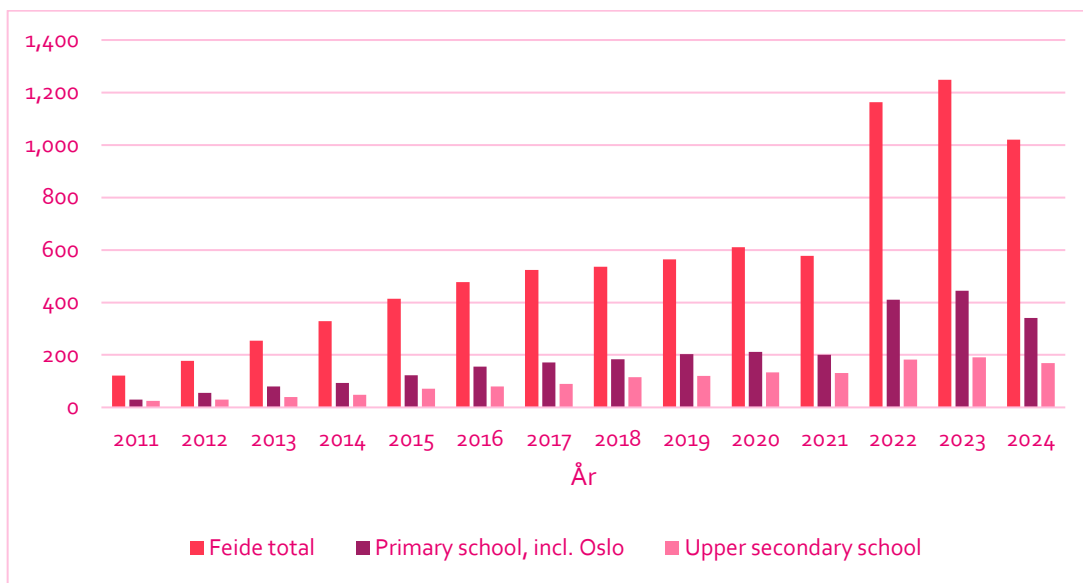


Figure 1 Total number of service providers linked to Feide (also divided into use in primary schools and upper secondary schools). 2024 numbers are for January.

In the education system, there is enormous data flow of information and *Feide* plays a key role in this dataflow (see p.9). In that sense *Feide* provides an overview of the dataflow and is connected to both persons and secure information. As Heidi explains: “some of the last things that we have been working on is actually to support the process of conducting risk assessments and entering into data processing agreements and all the things that every school owner [municipalities] is actually required to do in connection with using various digital services”. *Feide* has therefore become a platform where schools can use various digital services in a secure manner.

Richard which is representing one of the municipalities explains *Feide* as an important “identity manager”. *Feide* provides a common identity; that is, the vast majority of digital learning resources and services that students use at school, use *Feide* as a login and managing the identities of the users. For teachers, *Feide* enables secure login, and they have control over students' identities and who has access to which information.

As a representative of a school owner, Richard further explains how the municipality works continuously conducting risk analysis of the digital learning resources they use, seeking to do this

process simpler by for example including self-declarations from the providers or publishing houses regarding risk assessment. Eventually, these self-declarations are supposed to include information and answers that school owners can generate from the self-declarations. It means that when you as a host organisation (school or a municipality) enter through *Feide*, you should be able to access a learning resource and get answers to your questions from the self-declaration form the service provider has attached. The idea is to generate an initial risk assessment and initiate a data processing agreement. In the initiated data processing agreement, the host organisation (for example school) gets the opportunity to extract some data about the provider related to the data processing agreement. Richard concludes by saying: "you have to make part of the assessment yourself regardless of local conditions. You still hold the responsibility as the school owner, as the data controller. You cannot delete that part".

If a student moves to another municipality or transitions from lower secondary school to upper secondary school, or from upper secondary school to higher education, they will not keep the same *Feide* identity. The same applies to teachers who change workplaces, for example, from one university to another; they will receive a new *Feide* identity. The *Feide* identity is therefore linked to a *Feide* host organisation, such as a municipality, county, or private school. Roger even claims that *Feide* may be one of the biggest "digital success stories" within the education system in Norway. *Feide* was also an extremely important service under the Covid-19 pandemic. Even though many teachers and school owners managed to turn things around quite quickly (Gudmundsdottir & Hathaway, 2020), Richard explains that they would have struggled if it hadn't been for *Feide*. There would have been a lot of proprietary solutions for which school owners couldn't guarantee the same level of security for the students, as they were not able to conduct a thorough risk assessment of everything that was taken into use partly due to free access to digital platforms and teaching/learning resources provided by educational resource providers.

Feide has been steadily growing since its beginning and has become an important hub for students and teachers. *Feide* collects information about teachers under strict privacy regulations, including names, email addresses, and details regarding roles and affiliations. This data is exclusively utilized for access control and the personalization of digital services. *Feide* ensures that only the minimal essential personal information is shared with various services, in compliance with agreements between host organisations and service providers.

The data processing agreement for the use of *Feide* between a host organisation and Sikt includes several aspects to ensure privacy and information security:

1. Data controller: The host organisation is the data controller of personal information, while Sikt acts as the data processor.
2. Purpose: The agreement governs how personal data should be processed in relation to the use of *Feide* services.
3. Security measures: Requirements are in place for technical and organisational security measures to protect personal information.

4. Rights and duties: The agreement outlines the rights and obligations of both parties, including the procedures for handling data upon the agreement's termination.
5. Risk assessment: It mandates the conduct of risk assessments to identify and manage potential risks associated with data processing.

In Figure 2 below we see the SSO growth over the last years and also the division between primary education and upper secondary education logins. *Feide* has implemented a lot of automation. It is no longer necessary for a school owner or school leader to think about group/class/cohort and such things as the information is taken from the system i.e. school owner's/*Feide* host organisation's study administrative system/HR system (teacher/employee) and access in *Feide* is automatically generated explains Richard. The biggest challenge is that a few service providers have not adapted to this, so adjustments have to be made manually to roles and affiliations of the users. There are also challenges regarding foreign service providers or those outside the Nordic region that are in use in schools, but both Danish and Swedish providers have adapted to the *Feide* system.

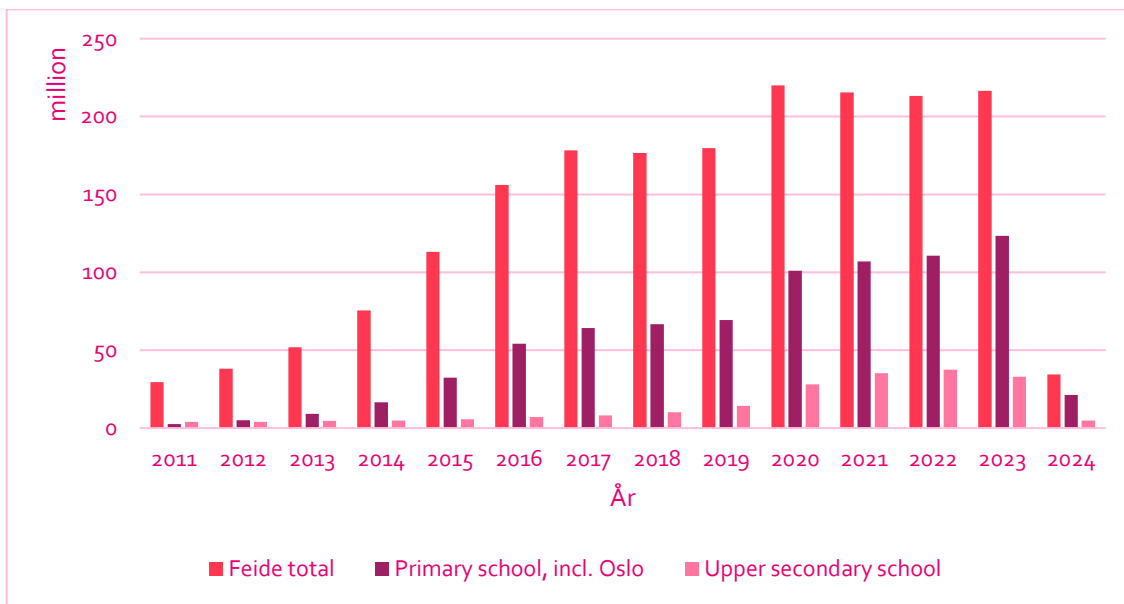


Figure 2 Total Feide single sign-in in million from 2011 – January 2024 (divided into providers to primary schools including Oslo and secondary schools)

As with any other technology there have been significant advancements in SSO services over the past decade. Our informant Heidi explains future developments within *Feide* and how this hub or ecosystem where different stakeholders are connected is important to view challenging aspects in the use of digital services. She mentions the issue of data flow "because digital services require information about the users, who the users are, what subjects they have, which class they belong to, what teachers they have, and what kind of school they attend."

A part of the development within *Feide* is also greater focus on risk assessment and data processing agreements and how *Feide* can support each school owner in this process. Previously, *Feide* did not address these aspects but as it has grown to be such a central hub within the education system it is becoming a more natural part of the *Feide* services. *Feide* has the central technical solutions whereas the municipalities have done great work to organize users, data flow, master data, etc. In that sense *Feide* can be seen as a platform that lowers the threshold for safe implementation of digital services in schools.

Data in use for teaching and learning

One of the latest developments within *Feide* is the so-called parental-pilot. This is a service meant for parents to get greater access to their child's schoolwork and therefore it is closely connected to *data in use for teaching and learning*. We will present how our informants describe the parental pilot and how they view its potential and challenges including the implications for teaching and learning.

Parental access

For many years, in a Norwegian context, there has been talk of parents needing better insight into and more information about their children's schoolwork. It has become more difficult for parents to have insight into their children's schoolwork since access is digital and no longer available in physical books. *Feide's* role is crucial when it comes to parental access. Heidi explains to us that *Feide* has the functionalities in place that are needed to give parents access, but the main issue is that both schools and service providers need to open up for parents and give them the opportunity to get insight.

Both schools and school owners notice greater engagement of parents and the need for more information regarding what happens in schools in the context of their child's learning. This is information that Richard relates to for example what resources or school books are the children using? How far have they come, and have they done all the assignments assigned by the teacher? In addition, it can be useful for those helping with homework to find out the thematic context of the assignment or what they have been doing in previous lessons at school. Finally, regarding assessment it can be useful for parents to take a look at assessment criteria and teacher's formative feedback on assignment when their child for example doesn't understand teachers feedback.

Roger tells us about the background of the parental pilot which is a public hearing on the *Feide* 2.0 specifications from 2018. This public hearing resulted in numerous contributions in various areas, one of which involved expanding functionality related to the parent-child relationship. It was noted that certain services provided *Feide* login (for students/employees) and separate login were used for parents (via ID-portal or similar platforms). In these cases, there was a need to establish the relationship between the student and their parents. As long as *Feide* (and the ID-portal or similar

platforms) do not contain information about this relationship, separate integrations had to be set up to connect students with their parents. The *Feide* service can primarily offer parents access to relevant data about their children, and similarly, students can see relevant data about their registered parents. Our informants name that *Feide* parental access is particularly relevant related to digital learning resources, learning platforms, communication solutions, registration, consents, and learning analytics/assessment applications.

The development of the parent-child API was proposed as one of the measures in the further development of *Feide* already in the *Action Plan for Primary and Secondary Education (2020-2021)*. It was then decided, in further detail, that this would be included as one of the measures in the future development of *Feide* to enhance school-home collaboration. As part of the process of establishing this new functionality, work was initiated to facilitate logins via ID-ports for parents. This was a time-consuming process, and it wasn't until spring 2022 that this functionality was possible. Participation in the parental pilot was on an invitation basis only. A number of municipalities of different sizes and complexities were invited to be a part of the pilot project.

Our informants explain the complexity of the parental access and emphasise that this is a project still in a piloting phase. "It is a small-scale pilot and afterwards, we will evaluate the pilot together with Sikt, the pilot municipalities, and the relevant service providers determine the possibility of further production deployment of the service in *Feide*", says Roger.

In 2024 Sikt and UDIR have expanded the work on the parent-child functionality to include any other *Feide* host organisation interested in being a part of the pilot. UDIR has been approached by suppliers considering using the parent-child functionality in their services and contact with publishers has been established. Such cooperation regards the opportunities for involving parents/guardians and other close relatives of the students in the use of their digital learning materials and services. This work is yet to be finalised and remains in process.

A part of the parent-child functionality is the development of a student-relationship map. Such mapping is a necessary part of the *Feide* parent-child pilot in order to define one or more new access categories for individuals related to students. Parental access was piloted in two municipalities by conducting a "parental survey" on well-being at school called *Klassetrivsel* (<https://klassetrivsel.no/>). This is a survey that has been conducted in several municipalities before, but using it together with parental access through *Feide* is new. The questions were grouped into themes (areas of investigation), for example 'class life', 'students' positions and relationships', 'grouping in the classroom' and 'the student's relationship with the teachers'. The pilot worked as intended. For one of the piloting municipalities, it is relevant to further explore how parental login can be used on other services, for example, to digital learning resources. Oslo, the biggest municipality in Norway has already started piloting *Klassetrivsel* in its schools and will conduct a trial of *Klassetrivsel* through *Feide* access. The trial will take place in selected schools and is currently planned to be conducted in the first months of 2025, initially in selected schools.

All these trials have revealed the necessity to include a new access category of close caregivers where students live in households with for example their older siblings or grandparents. The access

categories parents/primary guardian and responsible caregiver are defined in the Norwegian version of OneRoster. Current efforts to standardize the use of OneRoster aim to enhance data exchange and integration across various educational systems (OAS/SAS, digital learning materials, services, etc.), including the standardization of relevant access categories in the student relationship map.

Rights, regulations and privacy

In this section we will address questions that touch on rights, regulations and aspects of privacy for Feide users.

The current situation for parents and school children in Norway is that if parents want to access their child's schoolwork they must sit next to the child to view their schoolwork or use the child's Feide access information. Developing a parental access functionality is considered of interest for parents that are getting more and more engaged in school affairs. Parental access is contingent on the municipality's decision regarding what access rights parents should have. The educational resource provider then facilitates parental access, which allows parents to view student's submissions related to that specific provider, without the student needing to log in.

Developing parental access takes time and there are several legal considerations regarding what right parents have to get access to content, which content they should have access to and privacy of the student himself (see 4.1). Previously, we have mentioned aspects of who is defined as a child's parent/guardian, but parental access also involves regulations regarding how, where and what data is stored and data storage requirements in schools. This however all rests on data quality.

Data quality

According to Heidi the main challenges regarding the parental-pilot are related to data quality. She explains this as follows:

"We are completely dependent on the accuracy of the data entered in the system. If it's not accurate, we're going to face problems as well. It's a massive task because it involves the workflow at each individual school, often involving the correct registration of information in the school administrative systems. It's a tremendous challenge, one we generally face as well [not only regarding the parental access]. Because good data quality is crucial for students to have correct access and to be placed in the correct groups."

Inaccurate data can be information hand typed inaccurately or that data fields were wrongly defined, not appropriate for the person/user. Roger explains how the school owner is responsible for data quality in their source systems (educational and administrative systems, HR systems).

These systems are connected to *Feide* so that by ensuring correct information in the source systems, the school owner ensures that the right student, teacher, etc., gets access to the digital learning resource(s) they are supposed to have.

The issue of *data quality* is also intertwined with legal aspects, such as determining who holds legal responsibility for the child. An example highlighted in the interviews is when only one parent has legal responsibility for a child. Another challenge is how we define who is "a parent"? Does that include grandparents, siblings, stepparents, and other caregivers who may assist the child with their schoolwork and therefore may need access to the child's schoolwork and educational records?

The issue of what defines a 'parent' today compared to before is something Benjamin mentions specifically as a challenge with such a parental log-in. He explains:

"I have worked on this together with the Directorate of Education and Training, about the role of parents. Who are the parents? And what kind of granulation is needed there? Because there are so many different types of responsible parents. And in the digital this becomes very apparent. Because in practice, it is the person the student goes home to and [where he/she] sleeps that in practice is the parent, that has access to the school bag and write a notice in the old book to the teacher. In the digital world you are disconnected from that. So you need algorithms and routines that decide who is a parent and what kind of access they should have. In the first version of the implementation of parents in Feide it was either or to define parent and access. In our municipality we have created like a parent-tree with all kinds of possible variants of families and parents. "

Not to forget the child, which is also an active part in the parental access. Privacy issues and children's rights according to UN's *Convention on the Rights of the Child* need to be considered. Richard explains that some hold the opinion that formal parental access without the child involved is unnecessary and should remain as it is. This means that parents who today want to access the schoolwork need to sit together with their child and view the schoolwork on the screen alongside their child. There are several complicated issues regarding access and consent that need to be solved and formally it still has not been decided *who* should have access (see 4.1). As Richard states when seeking to map students' family and relationships: "the relational maps are quite extensive" and according to the child's age they will need to consent to their parental access. When the student is younger, the parents give consent for processing personal information, but as the student grows older, particularly from secondary school age, students gain more influence over what information is shared. Schools for example reduce access to sensitive information so that only authorised personnel have access. Data used for research or statistics is anonymised to protect student's identity.

Information about health-related matters and special needs education is treated with particular care and only shared with those who have a legitimate need to access the information. From

secondary school and onwards the school protects certain types of information from parents to safeguard student's privacy and autonomy. Information about student's health, including mental health, is shared with parents only if the student consents. In upper secondary school, the student can decide whether grades and assessment results are shared with their parents. Finally, details about absence may be withheld if there are sensitive reasons behind the absence that the student does not wish to share with their parents.

There are, however, those that see great potential of this work. Such mapping of data is related to legal aspects and quality of data which can have significant synergies in terms of school-home cooperation in other areas. This includes possible cooperation between different stakeholders including for example The Norwegian Directorate for Children, Youth and Family Affairs (Bufdir) which includes the Child Welfare Services (Barnevernet) and the Educational Psychological Services (PPT). This could, for example include vulnerable children with diverse needs, those in foster care, or those facing challenges like substance abuse or mental health issues. *Feide* could significantly improve the coordination and delivery of support services by centralizing access to information and streamlining communication and collaboration among various stakeholders, such as social services, healthcare providers, educators, and legal guardians.

In relation to such cooperation *Feide* could establish effective communication solutions between the homes and school which are secure and capable of handling sensitive information. Richard explains this as follows: it is about sensitive information which may involve multiple stakeholders in the "team around the student". One aspect are the students themselves, considering if it is necessary and appropriate for them [the parents] to have access, as they also have rights in terms of being involved". These are some of the challenges that our informants point at. Currently, there are no comprehensive solutions addressing these aspects.

Equal access – digital divides

Feide can also contribute in terms of equal access to data and digital tools. Heidi explains that implementing digital services requires a considerable amount of preparation, and municipalities have to handle many aspects on their own. It is not only the technical aspect, but primarily issues related to security and privacy. Small municipalities often struggle with these matters since they lack the expertise and capacity to conduct risk assessments and vulnerability analysis. As a result, they tend to have an open approach to everything, leading to less secure use of digital tools or else they shut down everything.

Among our informants we have different size municipalities represented. Benjamin and Kurt represent very different municipalities. Benjamin explains how his big city municipality needs to plan for scaling up involving a large number of schools and covering the whole trajectory from kindergartens to adult learning. While Kurt explains how they have to explore for ways if developing strategies without much of the legal and technological expertise that larger municipalities have access to and that larger municipalities also have better access to central national agencies like the Directorate of Education to be involved in strategy work.

When asked about possible *digital divides* in terms of access to data Richard answers that he believes that the average person in Norway is used to these types of SSO authentications. He continues:

They are used to SSO for example when it comes to logging into online banking or whatever you need to do. But of course, we have some who have always lived in Norway and others that are new to the country. So, the question is whether it will be a challenge regardless. If we look at the parents who now have kids starting in grade 1, let's say they are around 30 years old. The majority of these parents went to school themselves and experienced that computers were a part of their everyday life. This has been normal for them throughout their education. They are relatively computer literate. I think the biggest challenge is that everyone knows there is a lot of information available, but how to access information that is adequate? I believe that is a bigger challenge.

Richard also mentions the importance that everyone has the same rights, but that it inevitably is a difference in how people experience the accessibility of information. Some find it demanding whereas others do not have any problems accessing and using different services. The Directorate of Education and Training have assisted the pilot municipalities with general information related to the trial of services (Klassetrivsel - Parent Survey for example). The need for potential information meetings has been discussed, but formal training sessions for parents has not yet been considered necessary. Any future needs for training or information regarding the use of Feide's functionality will be considered based on the areas of application.

Parental Consent

A common issue that several of our informants mention which *Feide* could make easier is how to handle parental consent. It is for example necessary for schools to seek consent from parents regarding school trips, regarding taking pictures and publishing online on the school webpages etc. There is no existing central system for such consents, but there is definite need to address this and whether it can be addressed through *Feide*. In order for parental access to be beneficial for the parents, it must include enough information about student's learning that is made available and easily accessible for them, Richard concludes.

One of the biggest municipalities in Norway has developed a consent functionality that gives parents/guardians the ability to give consent for school photos, opt out of receiving iodine tablets, and consent for school transfers. The consent solution is locally developed by the municipality itself. In the parental pilot, there has been reported the need for a national consent functionality in connection with the use of the parental pilot.

There has also been reported the need for further development of the parental access functionality and defining close caregivers. This includes, among other things, mapping the needs to create

additional new access categories for individuals in relation to students. This is because it may be relevant to provide individuals in relation to the student with different access to information, functionality, and decision-making.

In the first instance, there has been identified a new access category – "close caregivers" Furthermore, the project includes insight and mapping work with school owners and other relevant actors concerning the existing and future needs for information, functionality, and decision-making in various IT solutions in primary education, the information and functionality and decisions various individuals in relation to the student should have access to. This work includes several complex legal and privacy-related clarifications.

Currently, parents and guardians have to deal with information exchange through different systems and communication channels used by the school owner. This can include information related to learning platforms, email, various mobile applications, physical letters, and phone calls. It should be noted that while the legislation sets limits on access to and information about the student as they get older (see further 4.1 & 5.1), there is a clear expressed desire from parents/guardians to have access to more information in order to provide the best possible support and assistance for their children says Roger.

Such kind of *Feide* use also addresses a need for renewed policies related to this type of functionality. Roger explains that this may include considerations for the child's age and different types of guardians, as well as establishing a best practice guide for the school owner. All this work must also be viewed in relation to the current legislation and privacy recommendations from the Norwegian Data Protection Authority.

| Data governance

Following the recent discussions about the use of screens and screen time in schools, there is an increased emphasis on ensuring that digital tools provide added value in schools. Students should feel both safe and secure, and we expect to see *added value* by the use of digital technology in education, says Roger. Therefore, data governance and quality of services is going to get more important. The work which is done in the municipalities on this is very important and the collaboration between the state (*Feide*) and administrations in the municipalities is crucial in order to get the expected ultimate outcome.

To use *Feide*, host organisations (schools, municipalities, universities) must establish data processing agreements with both Sikt and relevant service providers. In addition, risk and vulnerability assessment analyses (ROS) related to the use of digital learning resources and services must be conducted.

Thus, through the *Feide* service, the Norwegian Directorate for Education and Training and Sikt is assisting host organisations in improving and streamlining this work. One of the developments is to further improve the functionality in the *Feide* customer portal that facilitates the process of ROS

(risk assessment) and DBA (data processing agreement). Simplifying the process of conducting risk assessment analyses and establishing data processing agreements is important. Working with risk assessment (ROS) and data processing agreement (DBA) *Feide* aims to make it easier for host organisations to adopt new digital services. This work includes; first a risk framework that host organisations can use to assess risks related to specific services (ROS). This framework is a collection of risks added by selected host organisations. Second, all services that process personal data must have a data processing agreement between the service provider (data processor) and the host organisation (data controller). The project has created templates for data processing agreements to simplify this process. Lastly, service providers fill out a supplier declaration for information security and privacy, which host organisations can use in their assessments. These measures help reduce duplication of work and make it easier for both host organisations and service providers to conduct necessary assessments and agreements.

The work is carried out in collaboration between the Norwegian Directorate for Education and Training and Sikt, involving others such as the Norwegian Association of Local and Regional Authorities (KS), and KiNS - The Association for Municipal Information Security.

Further development of *Feide* contributes to ensuring that service providers can reach their users more accurately and *Feide* services are becoming more and more precise, so that school owners/municipalities can feel confident that the digital learning resource is easily accessible through *Feide* for the “correct” student and teacher who are supposed to have access and the particular service. Access to various resources can also be controlled on a school-to-school basis which means that not every school in the same municipality has access to the same digital resources and services.

Guidance and Support

When asked what kind of guidance and support schools need and get from school owners regarding the use of *Feide* and one of the municipality representatives' states that they don't really need any form of support. The only challenge is in case of *Feide* being down. Other than that, “*Feide* is pretty self-explanatory” (Richard). Nonetheless, one of the biggest challenges the representatives from the municipalities experience is related to two-factor authentication and the fact that teachers or school staff do not have their own mobile phones. Different municipalities have tried out different solutions, for example the use of codes and USB sticks. Some municipalities have provided teachers with mobile phones, while others allow the use of personal mobile devices. This shows that there are different arrangements regarding how two-factor authentication is addressed in the various municipalities. Another thing is whether the students themselves need a mobile for two-factor authentication and that is a greater challenge and connected to a much more controversial matter of whether students use of mobile phones should be allowed in school or prohibited.

Age of students is mentioned by several of the people we interviewed as a challenge and something that needs more national coordination. *Feide* was originally developed for universities

and soon also included schools. However, for the students during the first levels of schooling and even in kindergartens single-log-in is difficult. Some schools have students carrying QR-codes around their neck to be used when logging in, or they ask the teacher every time they need to log in for the password which is then the same for all. Both Benjamin and Kurt mention that this is something they have addressed with national authorities and something they are working on to find safer log-in procedures also for the young children in formal education settings.

The municipalities can seek advice from Sikt in terms of technical issues. Heidi explains that handling all the data flow is important for the schools, and *Feide* has several individuals who work with advising and guiding the schools and school owners. These can be questions ranging from how to use the functionality of the service to more specific technical issues.

Expert panel

Feide has an expert panel through which school owners can provide input to the development of *Feide*. The Directorate of Education and Training is responsible for the *Feide* expert panel. It is a professional forum for clarifying challenges related to the use, management, and further development and innovation of *Feide*. For instance, when new services such as the parental pilot are under construction, several municipalities willing to test and provide feedback during the service's development are included in the process. The Norwegian Association of Local and Regional Authorities (KS) is also represented in the *Feide* expert panel.

The persons in the expert panel are chosen from different stakeholders connected to users of *Feide* and they have varied background and competencies in terms of privacy, technical expertise, expertise from schools etc. When asked about the role of the expert panel Roger says that it: "highlights requirements from their own organisation and addresses issues/challenges on behalf of the education sector. This can include ideas, needs and proposals that cover a wide range within education, as well as challenges related to solving them. It may also involve the fact that *Feide* currently provides some of the functionality they desire, but further development is desired". The expert panel should represent a good cross-section of the users and competent individuals with extensive experience in their respective fields, who are active drivers, engaged, and motivated in terms of the development of *Feide*.

Commercial actors

Feide has limited collaboration with EdTech and providers of teaching materials and as one of our informants mentions - one of the best things of *Feide* is its neutrality as it is a public actor without commercial interests. "Best case scenario, they [Ed-Tech] are connected to development projects through our insights work with individual service providers involved in pilot projects" (Heidi).

Still, there are different commercial actors trying to get in to the schools, selling their products. Most of them are rejected since they need access to schools and students through the various

platforms in use. Very many of these commercial actors are denied access because they are just interested in getting hold on student data, says Richard.

This results in:

1. The integration supports secure authentication such as multi-factor authentication (MFA) to enhance security. This means that users can verify their identity using multiple methods, such as SMS, email, or authentication apps.
2. The possibility of setting up passwordless login, where users can log in using their mobile phone instead of entering a password.
3. Schools and educational institutions can centrally manage user accounts and access rights through Entra ID, simplifying administration.

Despite being serious actors, there are still many unanswered questions related to opening up for commercial actors to all the students in a municipality. Our informant Heidi explains:

we can see that the aspect of SSO is becoming less and less unique. We have received better solutions from the government, such as ID-portal, although it may not be suitable for young users [children] at the moment, they are on their way to developing solutions for them as well. And not the least, major cloud services provided by for example Microsoft and Google, which have large development units deliver very good login solutions that we also use.

Related to the influence of commercial actors we hear that several of our informants highlight that *Feide* users may mistakenly assume that teaching materials or teaching resources were you use *Feide* are automatically quality assured or approved for use by the educational authorities or school owners. Use of *Feide* does however not include any quality assurance or approval from educational authorities. As Heidi explains: "We do not conduct any form of verification. Eventually, we ask the service providers to answer some questions about information security, but there is no pedagogical assessment of the content as many may have assumed". In Richard's municipality they use log-in data more and more to monitor use of certain services in order to get an overview of number of users to pay for licenses and decide whether or not they should be renewed. Is there limited use of an educational resource, according to low SSO numbers, there is no need to renew the license for all the schools in the municipality. He continues by explaining that *Feide* SSO numbers may be used as an indication when considering the pedagogical quality of the resource because if it isn't used by the schools there may be a reason behind that.

Conclusion and key implications

In conclusion, the *Feide* case in Norway serves as an example of the benefits of a national SSO service in the education sector. By providing a secure and streamlined authentication process, *Feide* has significantly improved access to various digital services for both students and educators,

ultimately leading to increased efficiency and reduced costs. Furthermore, the implementation of two-step authentication has enhanced security, protecting user privacy and reduced the risk of unauthorized access.

The support for data sharing in *Feide* has not only simplified access to digital services but also allowed school owners to maintain control over the sharing of information. As a result, *Feide* has both benefited individual users and also the educational institutions and service providers, ultimately contributing to a more seamless and efficient education system in Norway.

Roger looks at *Feide* as a hub where host organisations, i.e., school owners, are provided with secure login for users, granting access to the digital learning resources and services that the school owner allows access to. He explains how the two-factor authentication and improved user-customized services are the strengths of *Feide*. "It is worth noting that projects on risk assessment and data processing agreement (ROS and DBA) will make it easier for host organisations to adopt new digital services within *Feide*. This is an example of a win-win situation in collaboration with service providers", Roger concludes.

Overall, the success of *Feide* highlights the potential of national SSO to streamline access to digital resources, enhance security, and ultimately improve the educational experience for students and educators. In Richard's words:

If you imagine all Norwegian educational resource vendors as an ecosystem, without any connection to each other but contained within the same circle, *Feide* is the gateway. However, for *Feide* to be a gateway, those who get the key must be registered and defined as a student or a teacher, or you must work in one of our schools in the municipality. If you meet these criteria, you will be granted *Feide* access. We also need to approve those who are allowed to be part of this ecosystem. As a result, some service providers may be excluded from the circle. Within this system, we will also discover that different schools use different educational resources registered within *Feide*. Thus, each individual school can be said to have its own ecosystem within the larger ecosystem.

It will be interesting to follow the developments around how service providers will be able to adapt to *Feide* and make it possible for the "team around the student" to communicate better together in a secure and save manner. At times, many actors need to communicate about each student, and that clearly necessitates some form of national common solutions which *Feide* could be a central part of.

Another potential lies in *Feide* in higher education institutions which gives a unique opportunity to leverage student data for academic research. Potentially *Feide* data could provide insights into pedagogical methods and educational outcomes. By enabling data sharing for research purposes, a collaborative ecosystem could be fostered between educational institutions and researchers. This collaboration could focus on understanding study patterns, evaluating the efficiency of digital tools, and even forecasting future educational trends. Researchers could explore correlations between digital engagement patterns captured via log-in data and academic performance. Such

insights could drive improvements in curriculum design, teaching strategies, and resource allocation, ultimately enhancing learning experiences and outcomes.

Key takeaways:

- SSO like *Feide*, as a national service, creates security and trust for all users and providers of content in handling of data.
- The pilot focusing on parents log-in is important since it opens up for closer cooperation between schools and homes as well as the possibility for parents to access their child's data
- A certificate of minimum requirements can be used to incentivise EdTech suppliers to follow guidelines that will facilitate data interoperability and data sharing with local/regional and national authorities and schools.

To conclude, all our informants spoke warmly about future possibilities connected to *Feide*. In Heidi's words she sees the ultimate goal of *Feide* to be "to eliminate all the barriers, which allows teachers to focus on using good tools in a safe and effective manner, compliant with pedagogical gains in the classroom while safeguarding privacy".

The insights of our informants have shed light on the multifaceted as well as potential benefits of *Feide* and as the education ecosystem continues to evolve, the successful implementation of *Feide* signifies the potential for national SSO to transform how digital resources are accessed, utilised, and shared within the education sector.

Equity and inclusion considerations

- Design access systems for all learners, including young children, students without personal devices, and those with disabilities or language barriers.
- Offer implementation support to underserved schools, with simplified onboarding, legal guidance, and training for institutions with less capacity.
- Include all family types in access design, by enabling flexible caregiver logins and ensuring that guardianship, custody, and cultural differences are respected.
- Ensure users understand their data rights, with simple, multilingual explanations of what data is collected, by whom, and how it is used or protected.
- Recognize that access doesn't equal meaningful and inclusive use, by supporting digital literacy for students and families with limited technology experience.
- Support secure collaboration among trusted adults, by enabling role-based data sharing that helps schools, caregivers, and support staff coordinate without breaching student privacy.

References

- Erstad, O., Gilje, Ø., Gudmundsdottir, G.B. Wagstaffe, R.B., Kumpulainen, K., Viberg, O., Williamson, B., Tondeur, J & Howard, S. (2024). Datafication in and of Education – a literature review (2nd ed), European Schoolnet. http://agile-edu.eun.org/documents/9709807/9862864/Updated+D2.1+Datafication+in+and+of+Education_090623.pdf/3a549d79-6d8e-4dc7-b556-f8745414ee39
- Gudmundsdottir, G.B. & Hathaway, D. (2020). “We Always Make It Work”: Teachers’ Agency in the Time of Crisis. *Journal of Information Technology and Teacher Education* 28(2), pp. 239–250.
- Pashalidis, A., & Mitchell, C.J. (2003). A Taxonomy of Single Sign-On Systems. In: Safavi-Naini, R., Seberry, J. (eds) *Information Security and Privacy*. ACISP 2003. Lecture Notes in Computer Science, vol 2727. Springer. https://doi.org/10.1007/3-540-45067-X_22



**Co-funded by
the European Union**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.