

The role and impact of Feide in Norwegian education

EXECUTIVE SUMMARY

30 June 2025

Context

This case study examines Feide, Norway's national Single Sign-On (SSO) service, which provides secure access to digital resources in the education sector. Managed by the Norwegian Agency for Shared Services in Education and Research (Sikt), Feide significantly enhances the efficiency and security of digital service use in education in Norway. With ongoing developments such as piloting parental access, Feide is positioned as a central hub for managing digital identities and facilitating collaboration among different stakeholders.

Feide's background and context

Feide's origin dates to the early 2000s, initially serving higher education for secure login purposes. It quickly became important to the broader educational ecosystem. The funding model for Feide involves host organisations, paying based on the number of users, while service providers manage integration costs.

Sikt oversees Feide, which connects over 1.5 million users to approximately 2000 digital services, and acts as a central hub facilitating identity management and secure access in Norwegian schools and in higher education. Feide's robustness was significantly tested and proven during the COVID-19 pandemic, enabling secure online schooling through its infrastructure. The system ensures only necessary personal data is shared, building on strong compliance with GDPR.

Despite Feide's strengths, challenges remain. Some service providers require manual adjustments for smooth integration, particularly non-Nordic ones. Feide is actively evolving to support risk assessments and data processing agreements. Its function as a central hub for data flow continues to grow, prompting strategic developments to enhance user safety and service efficiency.

Data in use for teaching and learning

Core to Feide's function is its commitment to data quality, ensuring that identity management is accurate and that privacy of the users is protected. Feide operates by maintaining stringent data processing agreements with host organisations, including municipalities/counties (the school owners) and universities, ensuring that personal data is processed securely and responsibly.

Challenges arise in verifying data integrity across educational administrative systems, highlighting the importance of a service such as Feide. The parental pilot represents a significant advancement in Feide's functionality, aiming to provide parents with access to their children's schoolwork. However, defining guardianship roles and managing diverse family structures within digital systems remains complex, influencing parental access. The parental pilot initiative acknowledges the importance of extended caregivers and more nuanced access categories. Collaborative efforts among school owners, service providers and educators aim to refine these processes, with broader implications for improved school-home cooperation and data-driven strategies.

Rights, regulations, privacy

Feide embodies a thorough framework for rights, regulations and privacy, which is crucial in managing digital identities. An integral component is maintaining high data quality to ensure accurate access and secure information sharing. Challenges include not only defining guardianship roles as mentioned previously but also verifying data accuracy within educational administrative systems.

Privacy concerns necessitate clear guidelines for who can access information and how. Feide encourages stringent risk assessments and data processing agreements to address these challenges.

Data governance

Feide excels in data governance, underpinning secure access to digital learning resources. Host organisations establish data processing agreements with Sikt and service providers to ensure compliance. Feide facilitates risk and vulnerability assessments, streamlining organisational processes and supporting efficient integration of new services. School owners benefit from comprehensive guidance and technical support, ensuring optimal use of Feide while addressing challenges like two-factor authentication.

Feide's neutrality and structured approach to data management highlight its effectiveness in fostering secure educational environments. The collaboration between national and local authorities further refines these processes which are central to the success of Feide, empowering schools to leverage digital tools confidently.

Recommendations

1. **Enhance parental access integration.** Further work on defining access categories and streamline consent processes, in order to enhance parent-school collaboration is needed.
2. **Prioritise data quality.** Implement checks within administrative systems to ensure accuracy in registered user data.
3. **Facilitate stakeholder collaboration.** Strengthen partnerships among national bodies, school owners (municipalities/counties), and service providers to further develop Feide.
4. **Regularly update privacy protocols.** Adapt privacy measures in alignment with evolving regulations and user needs, ensuring robust protection of sensitive data.
5. **Monitor and encourage service provider compliance.** Develop certificates acknowledging minimum standards for EdTech suppliers, ensuring alignment with data interoperability guidelines.

- 6. Advance research opportunities.** Explore collaborative opportunities to leverage Feide's data potential for academic research.

In conclusion, Feide's SSO service demonstrates the potential for transforming digital access management and privacy in education. By addressing challenges, securing data quality and promoting stakeholder collaboration, Feide can be further developed to support dynamic and secure educational environments. These initiatives underpin Feide's position as a possible model of national SSO service in a European education landscape.



**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.