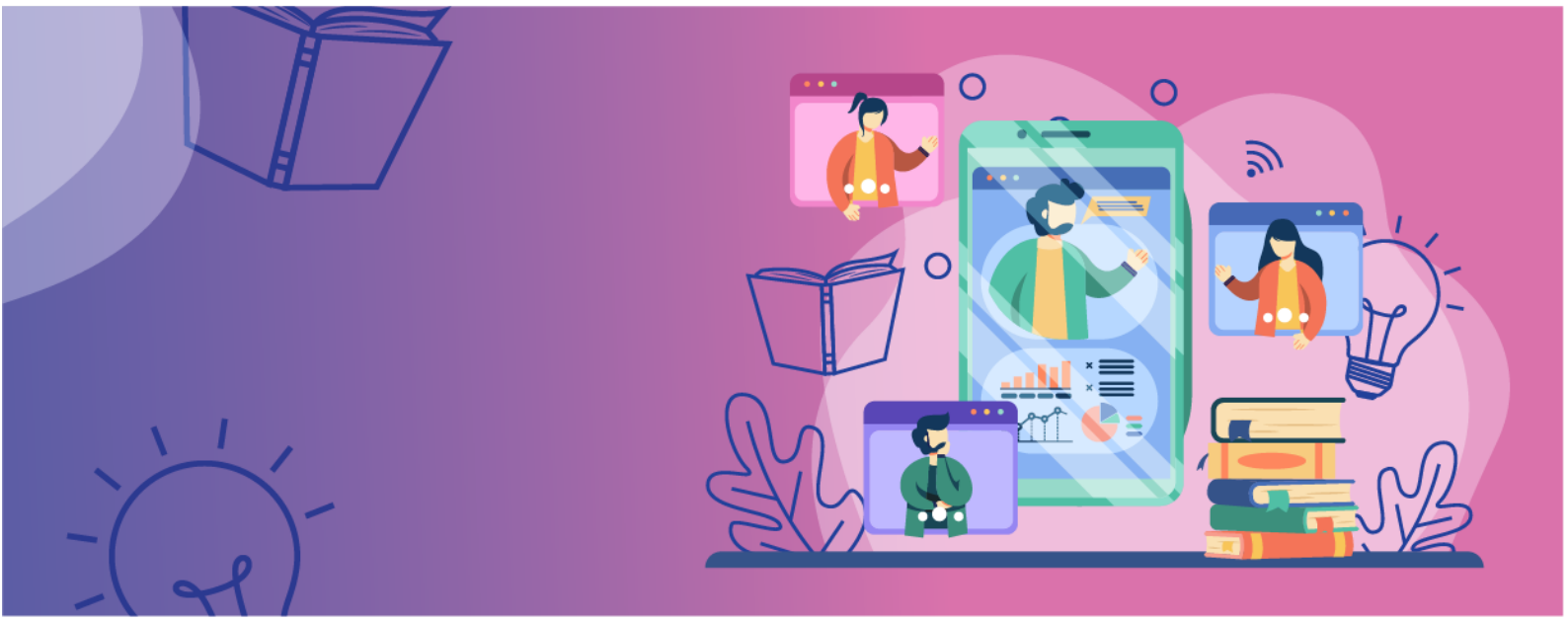
DIGITAL FIRST

Digital Tech as the First Language:

Informatics for Digital Natives

D7.4 Legal and ethical framework for safe educational data mining



Co-funded by
the European Union



Project 101132761

D7.4 Legal and ethical framework for safe educational data mining

Partner:	UTU
Work Package:	WP7: Data for success: Modelling learning analytics for informatics
Task:	T7.7 Discussing privacy and ethics challenges for using learning analytics for informatics in primary and secondary schools
Due date:	31/10/2026
Work package Leader:	UTU

Start date of project: 1 December 2023 **Duration:** 36 months

DOCUMENT HISTORY		
Version	**Date**	**Changes**
1.1	30/10/2026	

DISSEMINATION LEVEL		
PU	Public, fully open	X
SEN	Sensitive (limited under the GA conditions)	
CLASS	EU classified, confidential	

Co-funded by the European Union

MAIN AUTHORS	
Name	**Organization**
Daranee Lehtonen	UTU

QUALITY REVIEWERS	
Name (Quality Reviewer 1, Quality Reviewer 2)	**Organization**
Maja Šarić, Maja Brkljačić	Algebra University

LEGAL NOTICE

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.

© Digital First Consortium, 2026

Reproduction is authorized provided the source is acknowledged.

Co-funded by the European Union

PREFACE

Welcome to the third volume of our guidebook series on learning analytics (LA) in informatics education. Building on the foundational concepts introduced in Guidebook Part 1 and the topics of data modelling, visualization, and interpretation explored in Part 2, this edition addresses the privacy and ethical aspects associated with implementing LA in schools. Our aim is to equip educators and stakeholders with the knowledge and confidence needed to navigate the complexities of data-driven education in the digital age.

Who Is This Guidebook For?

This guidebook is intended for teachers, informatics professionals, researchers, administrators, policy-makers, and anyone interested in understanding how to handle educational data responsibly. Whether you're new to LA or looking to expand your expertise, this guide offers practical explanations, real-world scenarios, and straightforward advice in accessible language. While the focus is on informatics, the principles and frameworks presented apply to a range of educational environments.

Developed as part of the Digital First Project, this guidebook is the result of collaboration between the Turku Research Institute for Learning Analytics (TRILA) at the University of Turku, Finland, and a network of project partners. It draws on TRILA's expertise and findings from investigations conducted across ten partner countries: Bulgaria, Croatia, Cyprus, Finland, Greece, Italy, Lithuania, Portugal, Slovenia, and Spain.

Guidebook Part 3 comprises four chapters:

1. **Introduction to LA:** Summarizes what LA is, its significance, and its role in teaching, learning, and educational planning. For more details, see Guidebook Part 1.
2. **Student Rights, Privacy, Security and Ethical Challenges in LA:** Examines the legal and ethical dimensions of student rights and consent, as well as the privacy issues and ethical challenges involved in collecting and using educational data in Learning Analytics.
3. **Legal, Data Protection and Security Measures:** Examines the regulations, security protocols, and practical steps necessary to safeguard educational data.
4. **Responsible School Practices**: Offers guidance for establishing responsible and transparent practices within schools and other institutions.

How to Use This Guidebook

You are welcome to read this guidebook sequentially or to reference individual chapters as needed. Each section includes practical explanations and accessible examples. Technical terms are introduced gradually and clearly defined throughout to ensure ease of understanding.

Co-funded by the European Union

TABLE OF CONTENTS

PREFACE 1

1 INTRODUCTION TO LEARNING ANALYTICS 3

1.1 What is Learning Analytics? 3

1.2 Distinction Between Learning Analytics and Traditional Educational Assessments 3

1.3 Learning Analytics in K–12 Education 4

1.4 Learning Analytics in Informatics Education 4

References 5

2 STUDENT RIGHTS, PRIVACY, SECURITY AND ETHICAL CHALLENGES IN LEARNING ANALYTICS 6

2.1 Privacy, Security and Ethics in Learning Analytics 6

2.2 Student Agency: Rights and Responsible Data Practices 7

2.3 Personal Data 10

2.4 Risks and Challenges 10

References 14

3 LEGAL, DATA PROTECTION AND SECURITY MEASURES 16

3.1 Applicable Legal Framework 16

3.2 Data Protection and Security Measures 16

4 RESPONSIBLE SCHOOL PRACTICES 19

4.1 Pedagogy First and Human Judgement 19

4.2 School-level Governance 19

4.3 School Culture 20

4.4 Professional Development 20

References 21

Co-funded by the European Union

1 Introduction to Learning Analytics

Learning Analytics (LA) is transforming education by providing powerful tools to monitor, understand, and improve teaching and learning. At its core, LA involves measuring, collecting, analyzing, and reporting educational data with the aim of optimizing educational outcomes (Ferguson & Buckingham Shum, 2011; Shum & Ferguson, 2012; Nistor & Hernández-García, 2018). For a more detailed introduction, please see Guidebook Part 1.

1.1 What is Learning Analytics?

LA relies on "digital traces" generated when students interact with educational technologies—such as online platforms, learning management systems, and digital assessments. This means LA focuses on aspects of learning that are recorded electronically, enabling educators to turn raw data into actionable knowledge. These insights drive evidence-based decisions that enhance teaching effectiveness and support student learning.

The practical benefits of LA extend across various levels. For students, LA provides real-time feedback and personalized tasks that keep learning engaging and motivating. Educators are empowered to monitor individual progress, identify difficulties or misconceptions, spot early signs of disengagement, and adapt their teaching to meet individual needs. At the institutional level, LA supports curriculum planning, professional development, and quality assurance initiatives. By analyzing educational data, schools and universities can align strategies with evolving student needs and pursue continuous improvement.

Beyond everyday teaching, LA is valuable in educational research—analyzing large datasets to uncover how students learn, which methods prove most effective, and what factors shape educational outcomes.

The strength of LA comes from its interdisciplinary nature, combining educational theory, data science, and pedagogy. With tools such as statistics, machine learning, and data visualization, LA transforms complex data into actionable insights, including predicting student behaviors, evaluating learning outcomes, suggesting targeted interventions, and elevating overall educational quality (Yu, 2025; Awad et al., 2024). However, LA's impact relies not just on technical analysis, but also on effective interpretation, communication, and integration of results into everyday practices.

Recent advances in artificial intelligence (AI) have further strengthened LA's capabilities. AI enables rapid analysis of vast educational datasets, giving teachers and institutions deeper insights into student performance and engagement. Research shows that well-applied LA can significantly enhance student achievement (Awad et al., 2024).

1.2 Distinction Between Learning Analytics and Traditional Educational Assessments

Technological advancements are reshaping how student learning is assessed. Traditional educational assessments rely on standardized tests and teacher observations, offering only limited snapshots of achievement and often providing delayed feedback. These methods primarily focus on what students know or can do at the end of a lesson, missing the complexity and development within the learning process.

LA represents a significant shift. Instead of just tracking final outcomes, LA monitors the ongoing process of learning—such as engagement patterns, problem-solving steps, and time spent on tasks. This allows for timely feedback and formative assessment, enabling teachers to respond quickly to student challenges and adapt instruction as needed. LA provides a more holistic view by including factors like motivation, collaboration, and self-regulation, supporting broader educational goals beyond mere academic performance.

Additionally, LA uses predictive analytics to identify students who may struggle in the future, allowing for proactive support. Through personalized and adaptive tools powered by AI and big data, LA creates tailored learning pathways and feedback for each student. This transformation moves assessment from "one-size-fits-all" to approaches that recognize individual needs and strengths.

Ultimately, LA not only enables real-time monitoring and personalized interventions, but also fosters continuous growth and learner agency, aligning assessment practices with the demands of modern education.

1.3 Learning Analytics in K–12 Education

Interest in LA has rapidly grown rapidly worldwide, with increasing attention to its application in K–12 schools. While LA holds significant promise for improving engagement, personalizing learning, and supporting school decision-making, its use in primary and secondary education remains inconsistent and less developed than in higher education. Both globally and across Europe, schools face similar challenges—such as cultural and technological differences, practical barriers like limited teacher time, and the need for alignment with curriculum goals and classroom realities.

At the core, LA aims to equip teachers with data-driven tools for formative assessment, identifying at-risk students, personalizing instruction, and enhancing curriculum design. These efforts help educators respond to individual student needs, boost motivation, and encourage self-regulated learning. LA also supports school leaders with actionable data to inform decision-making, prevent dropouts, and improve quality assurance. A growing trend is the use of LA to facilitate transparency and collaboration, with real-time access for families to monitor their children's progress.

Despite its potential, successful LA implementation requires thoughtful adaptation to school contexts, stronger teacher engagement, and ongoing attention to practical and ethical considerations.

1.4 Learning Analytics in Informatics Education

LA has transformative potential in informatics education, where digital environments like programming platforms and simulations provide abundant data about student learning. Every coding attempt, problem-solving activity, or interaction with interactive tools is recorded as detailed digital traces, offering valuable information about each learner's process and progress.

These traces allow informatics educators to go beyond assessing final outcomes. LA helps teachers pinpoint where students encounter difficulties—such as debugging errors or misunderstanding concepts—so interventions can be targeted and timely. By analyzing student actions, LA reveals common error patterns and supports the proactive resolution of misconceptions, for example, in programming tasks. Moreover, LA assists in evaluating advanced skills like abstraction, decomposition, and algorithmic reasoning by capturing how students approach and solve computational problems.

Research demonstrates that integrating LA into informatics classrooms improves student engagement and performance, especially when combined with effective instructional strategies (Awad et al., 2024). Students benefit from timely, customized feedback, which keeps them motivated and supports deeper learning. Overall, LA enables more personalized, responsive teaching and helps both educators and learners gain meaningful insights into informatics learning.

References

Awad, I., ALGHAMDI, A., & Al-Farani, L. (2024). The Impact of Artificial Intelligence Technologies in Educational Informatics on Improving Learners Performance: A Meta-Analysis. *Journal of Umm Al-Qura University for Educational and Psychological Sciences, 16*(3), 349–364. https://doi.org/10.54940/ep41266805

Ferguson, R., & Buckingham Shum, S. (2011, February). Learning analytics to identify exploratory dialogue within synchronous text chat. In *Proceedings of the 1st international conference on learning analytics and knowledge* (pp. 99–103). https://doi.org/10.1145/2090116.2090130

Nistor, N., & Hernández-García, Á. (2018). What types of data are used in learning analytics? An overview of six cases. *Computers in Human Behavior, 89*, 335–338. https://doi.org/10.1016/j.chb.2018.07.038

Shum, S. B., & Ferguson, R. (2012). Social learning analytics. *Journal of Educational Technology & Society, 15*(3), 3–26.

Yu, H. (2025). Application of Learning Analytics Technology in Architectural Education Informatics. *Journal of Progress in Engineering and Physical Science, 4*(4), 31–37. https://doi.org/10.56397/jpeps.2025.08.04

2 Student Rights, Privacy, Security and Ethical Challenges in Learning Analytics

This chapter examines the key ethical and legal considerations in LA, beginning with privacy and data protection, and extending to student rights, consent, and responsible data practices—including the collection, storage, use, and sharing of educational information. Recognizing students as active agents in data-related decisions, the chapter also addresses the risks and challenges facing schools as they integrate LA into their practices. By exploring these dimensions, we aim to support the responsible and transparent implementation of LA that safeguards student interests and builds trust in educational contexts.

2.1 Privacy, Security and Ethics in Learning Analytics

Data Privacy

Data privacy, sometimes referred to as "information privacy," is the principle that individuals should have control over their personal data, including the right to decide how organizations collect, store, use, and share this information. In the context of LA, **personal data** may include a student's name, email address, grades, attendance records, digital activity logs, responses to online assessments, or patterns of engagement with educational platforms. Ensuring data privacy means students and their families retain the ability to make informed choices about who has access to this information and how it will be used within educational processes.

Educational institutions are legally required to respect data privacy rights, with regulations such as the European Union's General Data Protection Regulation (GDPR; EU, 2016/679) setting strict standards for how personal data must be handled and protected. Concerns arise when data is collected without adequate consent, stored insecurely, or shared in ways that compromise confidentiality, potentially exposing individuals to misuse or unauthorized access.

Data Security

Data security is essential for protecting educational data from unauthorized access, misuse, or tampering. In the context of LA, data security involves implementing robust controls—such as encryption, access management, and regular monitoring—to safeguard student information from both external threats and insider risks. Data security and data privacy are closely linked: security measures help ensure that only authorized individuals can access sensitive data for legitimate educational purposes, while privacy policies clarify who those individuals are and what constitutes valid use. Maintaining strong data security practices not only reinforces student privacy, but also builds trust among learners, families, and staff. Nevertheless, security concerns remain, especially regarding the risk of data breaches, hacking, or improper data handling that could expose personal information and undermine the integrity of LA systems.

Ethics

Research on ethical perspectives in LA consistently highlights key concerns such as protecting privacy and ensuring data security, transparency in data collection and usage, data traceability, unequal power dynamics in data gathering, individual awareness about how their data is collected and used in education, and obtaining consent for research purposes (Draschler & Greller, 2016; Pardo & Siemens, 2014; Sclater, 2016). Other important issues include clear principles and practices for data retention, the use of anonymization or pseudonymization, and proper data classification and management—often documented in privacy notices.

It is crucial to take into account the experiences and expectations of both data users and learners whose information is collected. This is especially important in developing effective LA applications and visualizations. Currently, data

used in LA is often fragmented, stored in multiple locations, formats, and standards, which complicates the creation of common ethical guidelines and increases the risk of misuse (Slade & Prinsloo, 2013).

Unethical data practices impact the entire educational environment by eroding trust between learners and staff or leadership. They can also lead to fear and prejudice against the use of LA. Therefore, when implementing LA at any educational level, it is vital to plan and apply a transparent and coherent data culture. This includes defining responsibilities, roles, rights, and anticipating negative effects, alongside adhering to data privacy and legal requirements. Beyond legal compliance, establishing principles and values for ethical use is essential. Ignoring ethical considerations can result in the failure of LA adoption. There may even be cases where the use of LA is lawful but is perceived by users as ethically questionable or undesirable.

2.2 Student Agency: Rights and Responsible Data Practices

Students are not merely passive subjects in LA systems; they are active agents with significant rights in how their data is collected, managed, used and shared. Recognizing student agency means respecting their right to be informed, to provide or withhold consent, and to participate in decisions about their personal information, while also being encouraged to use digital learning systems responsibly. Ensuring students—and, where appropriate, their families—have meaningful control over their data fosters trust and transparency, and is essential for responsible and ethical practices in educational settings.

Student Participation

Organizations may process student data within the scope of their legal responsibilities. For educational institutions, this typically means personal data processing is grounded in statutory duties related to organizing education, so consent is neither required nor recommended as the legal basis. As such, student agency in data use is best viewed as an ethical consideration rather than a legal one. Schools should communicate analytics results to students, encourage questions, invite challenges to interpretations, correct misinterpretation, and discuss how the data will be used to support learning. Providing students with opportunities to influence how their learning data are used not only strengthens the legitimacy of LA practices but also promotes their involvement in monitoring their own learning. Thus, LA should be used in collaboration with students, not merely applied to them. This is especially important in informatics education, where ethical data practices contribute to fostering responsible digital citizenship.

Ensuring equal treatment is a central principle in many educational contexts, including Finnish basic education. In Finland, LA is generally applied to all students within a group or not at all, thus upholding fairness for everyone (OKM, 2024). Additionally, Finnish students should have the option to opt out of analytics if there is a risk that the data could negatively impact their performance or educational experience (OKM, 2024).

Transparency

Transparency is essential when processing student personal data for LA. Students have the right to know, including:

- what data are collected, what are mandatory and what are voluntary;
- why they are collected;
- how the data are handled and used;
- who is responsible;
- who has access;
- whether data are analysed automatically;
- whether the system generates recommendations, predictions, or profiles;
- whether external providers process the data;

- how long the data are retained or the basis for retention;
- whether the data are transferred to other organisations or countries;
- what rights students and parents have;
- how decisions based on the data can be challenged.

If needed, this information must also be provided to student guardians. The same approach applies to teachers if data about them is processed.

Information must be provided in a clear, concise, and accessible manner, taking into account the age and language needs of students. For example, younger students may only need a straightforward explanation that their activity data is used to help teachers identify where extra support may be needed, rather than to rank their performance or to keep them under surveillance; while older students should also be informed about the limitations of analytics indicators and their right to question how their data is interpreted. For students whose primary language is not the language of instruction, information must be available in a language they can comprehend. Because LA combines data contributed by students with data from school records, students should be informed about both sources unless they have already received this information.

If LA involves profiling or automated decision-making, students must receive information about those processes, such as what data the algorithm uses, what rules or connections it searches for, and the weight given to various factors. Providers unwilling to share such information should be avoided.

Using a privacy notice is the most straightforward way to meet information obligations. For example, the notice can be shown on the user's screen the first time they use the service and whenever relevant details change. A read receipt, such as checking a box, can be used to confirm notice delivery. However, simply providing a privacy notice may not be enough for full understanding; both legal and ethical aspects of informing students should be considered.

Required permissions for LA

The most common purpose for using analytics data in education is to support teaching and learning. Processing students' personal data should primarily be based on the legal obligations of the data controller, the exercise of public authority, or the performance of tasks in the public interest. For this reason, processing personal data should not rely on the student's consent.

As a general rule, consent must be obtained for processing personal data when the educational institution offers additional services, such as leisure applications, to students or when the purpose is not related to organizing education. For example, LA data used for research is distinct from data used for educational purposes, thus requiring consent, even though research may also rely on other legal grounds. In practice, these objectives can sometimes overlap, so it is important to plan and communicate the intended use carefully in advance. The need for consent depends on the type of data and whether the information is pseudonymized or anonymized. However, Consent cannot be used as a legal basis for processing personal data in core teaching or education activities, as there is an unequal power relationship between students and educational institutions, making it difficult for students to provide fully voluntary consent. When data is collected with consent, students have the right to withdraw or discontinue their involvement according to research ethics. The right to object must also be respected when personal data is processed under the legal grounds of public authority or serving the public interest.

Minimization

Mere curiosity is not a valid reason for collecting or processing personal data. Any personal data used in LA must be necessary, relevant, and proportionate to achieving a lawful objective. It should be relevant and limited to what is

necessary, and must not be retained longer than required for those purposes. The principle of data minimization requires that schools avoid collecting data solely because an application has the technical capability to record it. Data that was not needed in traditional, paper-based tasks is likely unnecessary in digital environments as well—unless there is a clear and justified purpose (OKM, 2024). For example, log data may be an exception, but the requirement for necessity applies to the type, amount, and storage duration of data collected.

Inappropriate data collection includes gathering information that is not required for teaching, assessment, student support, or school records. Examples in a LA context are excessive monitoring, tracking students outside the learning platform, collecting irrelevant private communications, or gathering data for unclear profiling purposes.

Anonymity

LA practitioners should make it technically possible for students to hide their identities in certain situations. It is important to consider anonymity at different levels of activity—for example, data integration in background systems and the teacher's interface. Sometimes, students may prefer analytics to support their own learning, which changes how anonymity is handled.

Students should be able to control their own level of anonymity, including granting access to specific individuals, such as a school counsellor. Clear procedures should be established for such circumstances, along with justified reasons for the data's use. Access to combined data always depends on the individual's role.

In principle, students can choose to hide their data from public rankings. Most data processed through LA remains confidential, as it may reveal private aspects of a student's life and personal characteristics. Legally, pseudonyms are not required on course forums if discussions relate to teaching, but from an ethical perspective, offering anonymity in course discussions may benefit students who prefer not to use their real names.

Access and Control

Personal data ownership refers to a data management approach where individuals decide how their personal information can be further utilized. The aim is to empower people in a data-driven society, making it simple for them to access and benefit from their own data across different services. Current data protection legislation already gives individuals the right to access and obtain their own personal data, but personal data ownership seeks to make this data easily accessible, machine-readable, and transferable between services. For students, this includes all information collected about them as learners. When planning data collection, it is essential to consider the lifecycle of the data and communicate this clearly to individuals whose data is being gathered. In some cases, the law also sets the minimum retention period for data.

If a student exercises their right to access their data, they do not need to justify their request for access and should also be informed about other rights related to personal data processing. They have the right to request their personal data during this retention period, even after their formal relationship with the educational institution has ended (as long as the data is still stored). However, this right applies only to their own personal data. The information must be provided free of charge. A fee can only be charged for repeated or clearly abusive requests. Administrative burden related to data access can be reduced by offering privacy dashboards instead of relying solely on forms.

If a student's LA data has been irreversibly anonymized, it cannot be returned to them. Data protection regulations grant individuals the right to request removal of their personal data in certain cases. However, students usually cannot demand deletion of their information from LA systems as long as it is necessary for the organization of education. This right typically applies only if the data is processed unlawfully, is no longer needed, or is unnecessary from a teaching perspective. Dissatisfaction with academic performance or reluctance to use digital tools does not

justify deletion. If personal data is processed under the legal basis of performing tasks in the public interest or exercising public authority, students have the right to object based on their specific personal situation. Data must be erased if the institution cannot show a compelling reason for processing that outweighs the student's rights and freedoms.

2.3 Personal Data

LA involves processing data about students, teachers, or other users of digital learning environments. Personal data refers to any information that can directly or indirectly identify an individual, meaning privacy protection must always be considered in line with the EU General Data Protection Regulation (GDPR) and relevant national laws. In LA, the educational institution acts as the data controller, and service providers offering digital tools act as data processors.

GDPR also applies to pseudonymized data, which can be reconnected to individuals with additional information. Simply replacing names with numbers does not bypass privacy rules. Anonymous data, however, is not subject to GDPR; for example, group averages are considered anonymous if individuals cannot be identified, though care is needed when dealing with small groups.

Processing personal data includes activities ranging from collection and use to combining, deleting, or storing data—even passively. The rules apply regardless of whether the information forms an official register. Special categories of data, such as information on race, political views, or health, are strictly regulated and generally prohibited unless required by law and accompanied by robust safeguards.

Data use should be based on trust, transparency, access, consent, institutional responsibility, and clear educational benefit (Drachsler & Greller, 2016; Slade & Prinsloo, 2013). Data controllers are responsible for ensuring the security of personal data through appropriate technical and organizational measures. Public institutions must follow additional guidelines for data management and information security.

It is a misconception that GDPR prohibits the use of LA. Instead, it sets boundaries and requirements for handling personal data, ensuring LA is used safely and lawfully.

2.4 Risks and Challenges

Research into the ethical aspects of LA has revealed a range of risks and challenges that require careful attention (Sclater & Bailey, 2026). These include the protection of privacy and data security, transparency in data collection and use, and the need for reliable data traceability. Issues such as unequal power dynamics in data gathering, fostering individual awareness about data practices, balancing the utility of analytics with privacy safeguards, and preventing unintended data exposure are all critical concerns. Additionally, obtaining informed consent from students, particularly when data is collected for research purposes—remains a key ethical consideration in the responsible use of LA.

Balancing Pedagogical Monitoring and Student Privacy

A significant challenge for school management and teachers is determining the boundary between legitimate pedagogical monitoring and the infringement of students' privacy and autonomy. While monitoring student activity can support learning, provide early intervention, and improve classroom outcomes, there is a real risk of crossing into unnecessary or intrusive surveillance. The difficulty often lies in deciding how much data is appropriate to collect, how it will be used, and at what point monitoring begins to undermine student trust, independence, or sense of security. Without clear guidelines and shared understanding, teachers may struggle to distinguish supportive practices from invasions of privacy. To mitigate this challenge, schools should establish transparent policies,

regularly review monitoring practices, and engage students and parents in discussions about data use, privacy, and autonomy.

Surveillance

One of the primary ethical concerns in LA is the risk of shifting from supportive monitoring to continuous surveillance. While analytics can be valuable for helping teachers identify students who need extra support, constant tracking of activities—such as login frequency, response times, grades, behavior, and engagement—may create a negative environment where students feel persistently observed and judged (Slade & Prinsloo, 2013). AI-driven personalized learning systems pose significant privacy risks, as they often analyze academic records and behavioral patterns to create detailed learner profiles.

This risk is particularly relevant in informatics education, where debugging often involves trial-and-error and alternative problem-solving approaches. A student who generates many errors may be struggling, but may also be demonstrating persistence or exploring different strategies. If an analytics system interprets error counts, completion speed, or time spent online as direct measures of competence or effort, it risks misrepresenting the learning process. Therefore, such indicators should be viewed as prompts for dialogue and support, rather than as final judgements about a learner's ability.

This issue is especially critical for children, since educational records can shape their long-term digital identity. Data generated when a student is in primary school could be stored within institutional or commercial platforms for many years. To address these risks, schools must take a responsible approach, clearly distinguishing between information that genuinely supports learning and information that is merely used for increased surveillance.

Data Security Risks

Before processing personal data, educational institutions, as data controllers, must assess the risks involved, as required by GDPR. This includes evaluating the nature, scope, context, and purpose of data use in LA, especially given its role as a newer technological tool. Relevant risks may stem from the power imbalance between institutions and students, combining data from various sources, or evaluating student performance. Potential harm includes physical, mental, material, or intangible damage, such as private writing assignments being exposed to other students, leading to discrimination or bullying.

A data security breach happens if personal data is destroyed, lost, altered, accessed, or disclosed without authorization. GDPR requires documentation of such events and, in certain cases, notification to the Data Protection Ombudsman or affected individuals. Not all breaches are hacks; many result from careless handling or insufficient staff guidance, for instance, sending a report card to the wrong person.

Once risks and their likely consequences are identified, appropriate technical and administrative measures must be implemented. These may include pseudonymization, encryption, and staff training. Documentation of these actions is crucial. If risk assessment criteria specified by GDPR or the Data Protection Ombudsman are met, a Data Protection Impact Assessment must be conducted before starting processing.

As data controllers, educational institutions are responsible for ensuring their LA service providers do not compromise data security. Security measures must be confirmed before implementation, and institutions are liable for consequences if they fail to fulfill these responsibilities.

Sensitive & High-risk Data and Profiling & Labelling

Sensitive and high-risk data in LA require careful handling and clear distinction from routine administrative or sociodemographic information. Examples of such sensitive data include details about school social action, Individualized Education Plans (PEI), Special Educational Needs (BES), Specific Learning Disabilities (DSA), inclusive education measures, social vulnerability information, health data, biometric data used for unique identification such as facial recognition, racial or ethnic origin, mother tongue, family income, and other sociodemographic indicators used to characterize the school population.

While these data may be legitimate for administrative and statistical purposes, merging administrative records with detailed behavioural data can result in a far more intrusive student profile than either dataset alone. Therefore, they should normally be excluded from routine LA. Using sensitive data for analytics can risk creating unintended profiles, labelling (e.g., "at risk", "disengaged", or "low performing"), or introducing bias into analyses, which may impact students unfairly or lead to discriminatory outcomes. Therefore, educators and administrators must thoughtfully assess the purpose and ethical implications of including high-risk data in LA, ensuring safeguards to prevent misuse and protect student rights.

Inequality

LA algorithms rely on data, but if that data reflects existing social or economic inequalities, the resulting models may inadvertently reproduce or reinforce those disparities. For example, students may vary in their access to devices, reliable internet, quiet study environments, and digital resources. Students from rural or economically disadvantaged communities are likely to generate different digital engagement patterns than their better-resourced peers. This creates a risk that low digital engagement might be incorrectly interpreted as low motivation or ability, rather than as a consequence of limited access to technology. Addressing these challenges requires careful evaluation of both data sources and context before drawing conclusions about student performance or engagement.

Bias

Bias in LA can especially impact students with disabilities or special educational needs, multilingual learners, and groups underrepresented in computing. Historical data may reflect past educational inequalities, and small or unrepresentative datasets can make predictions unreliable or skewed. In digital analytics, indirect indicators like logins, clicks, views, or time spent on a platform can be especially problematic. These metrics do not directly measure student knowledge—since a student might work offline, use alternative resources, have unequal access to technology, or simply require more time to complete tasks. Risks are minimized when LA is integrated into high-quality formative assessment that uses clear criteria, multiple evidence sources, personal dialogue with students, and takes individual circumstances and progress into account. Analytical results should serve as a starting point for review and support, not as a final label or basis for automatic classification.

In AI-supported analytics, biased data can lead to predictions or recommendations that disadvantage certain groups (European Commission, 2026). Before using any analytical model to recommend support or identify student risk, schools should critically examine whose data underpin the model, which variables influence its outputs, whether error rates are consistent across different groups, and what safeguards are in place if the model makes mistakes. This due diligence is essential to prevent the reinforcement of inequalities and ensure fair, accurate outcomes for all learners.

Student Autonomy and Authentic Learning

A further ethical challenge in LA is the impact on student autonomy and authentic engagement. When students are aware that every interaction with an educational platform is being analysed, they may alter their behaviour to appear more engaged, acting out of concern for monitoring rather than genuine interest in learning. This can undermine the development of self-directed learning and intrinsic motivation.

Gamification, while often intended to motivate learners, may further incentivize students to focus on improving measurable performance indicators—such as earning points, badges, or completing tasks—at the expense of deep understanding. Certain AI-driven personalized learning systems can encourage short-term engagement and superficial achievement metrics, creating a disconnect between what is measured and true learning progress.

Schools must therefore recognize that "more data" does not necessarily mean "better education." It is essential to distinguish between meaningful educational activity and behaviour produced primarily for analytics purposes, and to foster environments where students feel empowered to learn authentically. Encouraging reflection, critical thinking, and meaningful dialogue about learning analytics helps ensure that data-driven approaches support, rather than limit, student autonomy and educational growth.

Transparency and Data Awareness

Insufficient transparency about what data are collected, how they are analysed, and who can access them is a significant risk in LA. When students, families, and educators are not clearly informed about data collection practices and analysis methods, it can create confusion, mistrust, and reluctance to participate. Lack of awareness undermines meaningful consent, prevents students from exercising their rights, and can lead to misconceptions about how data-driven decisions are made. Furthermore, when access to data is not clearly defined, there is a risk that sensitive information may be exposed to unauthorized parties, increasing the possibility of misuse.

To address these challenges, schools and institutions should communicate openly and regularly about data practices. Providing clear, accessible information about what data are collected, how they are used, and who has access helps build trust, enables informed consent, and supports responsible use of LA.

Reductionism

A related challenge is reductionism—the tendency to prioritize what is easily measured over what truly matters in education. LA often emphasize metrics like clicks, scores, response times, completed levels, or the number of submissions. While these provide some evidence of activity, they fall short of capturing deeper qualities such as understanding, creativity, collaboration, ethical reasoning, or the ability to transfer knowledge to new contexts. This issue is especially relevant in informatics education, which goes beyond technical performance and also involves functional, creative, critical, and responsible use of digital technology. Schools must be cautious not to let analytics reduce complex learning outcomes to simple metrics, and should seek ways to value and assess the broader dimensions of student growth.

Teacher Readiness

Teachers have recognized the potential benefits of LA, such as deepening their understanding of student participation and performance, providing meaningful feedback, and supporting self-regulated learning. However, significant barriers remain. These include increased workload and effort, limited data literacy and self-efficacy, insufficient support structures, and the need for broader cultural change in schools. To be truly effective, LA must be actionable, explainable, human-centred, and ethical—rather than simply offering additional dashboards without practical guidance.

Even a technically compliant LA system can fail ethically if teachers do not fully understand its outputs or lack the time and resources to act on them. Professional development should go beyond basic software training to include interpretation of data, understanding statistical uncertainty and bias, principles of privacy and cybersecurity, and effective communication with students and parents. School leadership must also ensure that analytics do not become an extra reporting requirement disconnected from classroom improvement. Without these supports, LA risks becoming a source of frustration or misunderstanding, rather than a tool for enhancing teaching and learning.

Over-Reliance on Automated Analyses

One important risk in LA is over-reliance on automated analyses at the expense of professional judgement by teachers. Algorithms may identify patterns or flag students for intervention based on digital data, but these recommendations can overlook context, individual circumstances, and nuances that educators are best positioned to understand—for example, disproportionate effects on students with disabilities or special educational needs. Excessive trust in automated insights may result in teachers feeling disengaged from the decision-making process, which becomes influenced more by algorithmic predictions than by individual circumstances. This over-reliance can lead to educational choices based solely on quantitative indicators, rather than embracing a holistic view of student needs.

Such over-reliance has the potential to diminish the teacher's role as an expert and mentor, and may increase the likelihood of errors or unfair outcomes, especially when automated models make inaccurate assumptions or reflect bias. While automated evaluation can, at times, be more objective than teachers, who may have personal biases or preconceptions that influence their judgment, human oversight remains essential. To mitigate this challenge, schools should view analytics as a support tool rather than a replacement for professional judgement. Encouraging teachers to critically evaluate automated analyses, supplement them with their own insights, and maintain active involvement in student support decisions ensures that learning analytics serves as an aid to, rather than a substitute for, educational expertise.

References

Drachsler, H., & Greller, W. (2016). Privacy and Analytics – it's a DELICATE Issue. A Checklist for Trusted Learning Analytics. *Proceedings of the 6th Learning Analytics and Knowledge Conference* (pp. 89–98). New York, NY: ACM. https://doi.org/10.1145/2883851.2883893

European Commission, Directorate-General for Education, Youth, Sport and Culture. (2026). *Guidelines on the ethical use of artificial intelligence and data in teaching and learning for educators* (Rev. ed.). Publications Office of the European Union. https://doi.org/10.2766/7967834

Ministry of Education and Culture, Finland (OKM), Learning Analytics Division. (2024). *Framework for Learning Analytics: Best practices in the implementation and utilisation of learning analytics*. https://urn.fi/URN:ISBN:978-952-263-731-4

Pardo, A. & Siemens, G. (2014). Ethical and privacy principles for learning analytics. *British Journal of Educational Technology, 45*(3), 438–450. https://doi.org/10.1111/bjet.12152

Sclater, N. (2016). Developing a code of practice for learning analytics. *Journal of Learning Analytics, 3*(1), 16–42. https://doi.org/10.18608/jla.2016.31.3

Sclater, N., & Bailey, P. (2026, September 9). *Code of practice for learning analytics*. Jisc. https://www.jisc.ac.uk/guides/code-of-practice-for-learning-analytics

Slade, S. & Prinsloo, P. (2013). Learning Analytics: Ethical issues and dilemmas. *American Behavioral Scientist, 57*(10), 1510–1529. https://doi.org/10.1177/000276421347936

Co-funded by the European Union

3 Legal, Data Protection and Security Measures

This chapter examines the legal frameworks, data protection requirements, and security measures essential for the responsible use of Learning Analytics in education. By understanding relevant laws, safeguarding personal data, and implementing effective security practices, schools and institutions can ensure that analytics tools are used both safely and ethically, protecting the rights and privacy of students and educators alike.

3.1 Applicable Legal Framework

Among the ten European partner countries, no national regulations specifically address Learning Analytics in schools. Instead, the use of LA is governed by broader legal and data protection frameworks that apply to school operations, personal data—including children's data, digital systems, and, where relevant, AI-supported tools. The primary legal framework is the **European Union's General Data Protection Regulation (GDPR**; Regulation EU, 2016/679), complemented by each country's acts implementing GDPR. Under these rules, schools act as data controllers and must ensure personal data is collected and processed lawfully, fairly, transparently, and securely. This requires schools to justify the purpose of data collection, limit what is gathered to what is necessary, and protect data against unauthorized access or unsafe sharing.

A **Data Protection Impact Assessment (DPIA)** must be conducted before undertaking any data processing activity that is likely to present high risks to individuals' rights and freedoms. This assessment is especially important in educational settings, as processing large-scale data and the personal data of minors—including for scientific research purposes—is explicitly recognized as a high-risk activity. A DPIA involves evaluating the nature, scope, context, and purpose of the data collection and identifying potential risks and strategies to mitigate them. By carrying out a DPIA, schools and institutions can proactively address privacy and security concerns, demonstrate compliance with legal requirements, and protect the interests of students and their families.

Increasingly, as AI technologies are used within LA systems, the **EU's Artificial Intelligence Act** (Regulation EU, 2024/1689) is also relevant. AI systems used for educational purposes—such as evaluating learning outcomes, determining student access or placement, or making other decisions with significant impact—may be classified as high-risk under this regulation. In such cases, schools and institutions must comply with stricter requirements related to risk management, transparency, data governance, and human oversight to ensure that these AI tools are used responsibly and ethically within education.

3.2 Data Protection and Security Measures

The EU's GDPR and other relevant regulations set forth principles including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability. These principles underpin key data protection and security measures, ensuring that personal data is handled responsibly and safeguarded in educational settings.

Responsible **data management** begins with deciding which data is genuinely necessary to collect, ensuring each digital or non-digital record—such as assessment results, LMS entries, teacher observations, rubrics, or portfolios—is linked to a clear pedagogical or legal purpose. Collecting data simply because it is available or easy to record creates unnecessary risks and undermines privacy. Schools must ensure data gathering always supports teaching, learning, or legal compliance.

Responsible LA also requires thoughtful governance across the entire **data lifecycle**, from collection through storage, access, sharing, and retention to final disposal. At each step, attention must be given to what data are collected and

why they are collected, how they are stored, accessed and shared, and how long they are retained. Ultimately, the process concludes with appropriate deletion, anonymisation, or archiving, ensuring data is handled with integrity and respect for privacy throughout its lifetime. Guidance on each phase of the lifecycle will be provided in later sections.

To ensure **transparency, accountability and compliance**, schools should document their purposes, lawful bases, responsibilities, access permissions, retention policies, and data sharing arrangements. Schools must establish clear procedures for data processing. Data should be collected for well-defined purposes, such as supporting teaching, learning, or research. Purpose limitation is essential: data gathered to enhance student learning must not be repurposed for unrelated activities, including disciplinary monitoring, commercial profiling, marketing, or public comparison of student performance. Adhering to these principles helps protect student privacy, maintain trust, and ensure the ethical use of data within educational settings. Students and parents must be provided with clear privacy information and an accessible process to exercise their rights. Records should clearly differentiate completed measures from planned improvements.

Data minimisation should be a fundamental principle in school-level LA. Schools must take care not to collect more information than is needed for educational purposes. In informatics education, digital platforms can produce highly detailed activity traces—such as time spent on tasks, number of attempts, errors, interactions, use of hints, progress, collaborative behaviours, and submitted work. While much of this data may be valuable, it should not be collected or stored indiscriminately. The key consideration is not what the platform is capable of collecting, but what information is truly necessary to enhance student learning.

Security measures should include the use of individual institutional accounts with strong authentication, encryption where appropriate, role-based access controls, secure storage instead of personal cloud accounts, and backups, software updates, restricted permissions, and clear guidelines for who can access student data (role-based access). Teachers should only access information relevant to their teaching responsibilities, while school leaders and administrative staff should be limited to aggregated or role-specific data. Unnecessary data sharing is prohibited. Schools should establish clear procedures for identifying and responding to security incidents. Researchers and external partners should work, whenever possible, with anonymised or pseudonymised datasets to further protect student privacy.

It is important to clearly distinguish between **anonymisation and pseudonymisation**. Anonymised data cannot be used to identify individual students and are preferable for generating reports, sharing research results, or conducting aggregated institutional analysis. Pseudonymised data, on the other hand, lower the risk of identification but are still considered personal data if re-identification is possible. In LA, pseudonymisation may be required when teachers need to link data to specific students for individual support; however, such data should be safeguarded with more stringent access controls and limited retention periods.

Data retention is a critical concern in LA. Schools should have clear policies specifying how long LA data are kept and when they will be deleted. Digital traces should not be stored beyond their educational purpose. For instance, quiz data used to adjust a lesson may not need long-term retention, while formal assessment records may be kept in accordance with the school's usual retention guidelines. Detailed behavioural traces should not be stored long-term unless there is a justified reason and proper safeguards are in place.

Schools must exercise particular caution when implementing LA through **third-party platforms and EdTech vendors**. Commonly used tools include Moodle, Canvas, Google Forms, educational games, classroom response systems, and

digital portfolio platforms. Before adopting any such tool, schools should carefully assess the provider's GDPR compliance, collected data, data storage locations, security measures, incident notification, data access, retention periods, auditability, and procedures for deletion or return of data following termination of use. It is also critical to confirm the rights of students and parents, whether international data transfers occur—recognizing that transfers outside the European Economic Area require a valid transfer mechanism—and whether student data are used for commercial purposes. Additionally, schools should ensure that platforms offer clear options for data deletion and provide sufficient transparency about their analytics processes. Importantly, a provider's claim that its platform is "GDPR compliant" does not substitute for thorough evaluation and due diligence. When a provider processes data on the school behalf, a written agreement should specify instructions, confidentiality and security requirements, procedures for supporting data subject rights and responding to incidents, arrangements for data return or deletion, and audit rights.

When **LA systems incorporate AI or automated decision-making**, additional safeguards are necessary. The EU Artificial Intelligence Act sets out a risk-based framework for AI, imposing specific requirements on high-risk systems—especially those affecting access to education, assessment, or educational pathways. Key principles from this framework emphasize human oversight, educational purpose, transparency, the use of authorized AI systems, and restrictions on practices that may impact student rights or enable inappropriate profiling. As such, predictive systems used in education to identify risk, recommend interventions, or influence decisions must remain transparent, explainable, and always subject to human supervision. Automated outputs should support, but never replace, the professional judgement of teachers and school teams. The Act also prohibits certain AI practices, such as using AI systems to infer emotions in educational institutions, except for specific exceptions outlined in the Regulation. This is especially relevant for LA, as systems that attempt to determine whether a student is bored, attentive, motivated, anxious, or emotionally engaged by analysing facial expressions, voice, behaviour, or biometric information raise significant privacy and ethical concerns.

Schools should evaluate whether a **data protection impact assessment (DPIA)** is needed, especially when processing involves large volumes of sensitive data, systematic profiling, AI, or vulnerable groups such as minors. Even if a formal DPIA is not legally required, conducting a basic risk analysis before implementing LA tools is essential. This review should consider the types of data collected, risks to students, access permissions, third-party involvement, retention periods, potential bias, and safeguards against misuse. A DPIA should go beyond a checklist and include a thorough evaluation of whether the use of analytics is necessary, if less intrusive options are available, what risks students might face, and how any potential harms would be prevented or managed.

All personal **data breaches** must be documented. Where notification is required, the supervisory authority must be informed without undue delay, and ideally within 72 hours of discovery. In the case of high-risk breaches, affected individuals may also need to be notified.

In summary, robust data protection and security measures are essential for responsibly managing LA. By adhering to legal requirements, implementing clear procedures, and maintaining effective safeguards, schools can protect student privacy and ensure data is handled ethically throughout its lifecycle. These practices not only reduce risks but also build trust among students, families, and educators, supporting the positive use of LA in education.

Co-funded by the European Union

4 Responsible School Practices

Chapter 4 focuses on responsible school practices for the use of LA. It offers practical guidance for educational leaders, teachers, and staff on how to implement LA ethically and effectively, ensuring student privacy and building trust. Schools, as data controllers, are responsible for the lawful, fair, transparent, and secure processing of personal data, while teachers must ensure that only accurate, relevant, and necessary information is entered and that LA is used exclusively for pedagogical purposes—never punitively or discriminatorily. Confidentiality should be maintained, and primary evaluation should always include human judgment ("human-in-the-loop"). Responsible use of LA requires more than legal compliance or technical security; it involves strong pedagogical judgment, institutional coordination, and clear governance to safeguard the rights and well-being of all students. By establishing effective policies, fostering transparency, and involving all stakeholders in data-related decisions, schools can harness the benefits of learning analytics while maintaining ethical standards and accountability.

4.1 Pedagogy First and Human Judgement

The first responsible practice is to clearly define the educational purpose of LA before collecting any data Analytics adds value when it supports teachers and students in understanding learning progress and planning effective next steps, rather than letting data collection become the primary focus. LA should be used primarily for formative and supportive goals, such as identifying learning challenges, adapting instruction, providing timely feedback, enhancing learning environments, and helping students reflect on their progress; instead of used to label students, make final decisions automatically, or reduce students to performance profiles.

Digital indicators and non-digital evidence should not be regarded as objective truths; they must always be interpreted in context and considered alongside student work, teacher observations, dialogue, feedback, formative assessments, and an understanding of each individual learner. No single indicator—such as infrequent LMS logins, slower task completion, limited oral participation, or an isolated observation—should automatically be used to judge a student's motivation or determine grades. While LA supports a data-informed, student-centred approach, it should never replace teachers' professional judgement. Educational decisions should ultimately be made by qualified human professionals who understand both the individual learner and the classroom context.

In informatics education, LA can provide teachers with valuable insights into how students approach programming problems, interact with digital tasks, use hints, debug errors, and progress through computational thinking activities. Errors, retries, and failed attempts often reflect productive exploration rather than a lack of competence. Therefore, it is essential to interpret this information as evidence of learning, not as absolute measures of ability or potential. By grounding LA in educational objectives, teachers ensure that data-driven approaches genuinely support student learning and development.

4.2 School-level Governance

Every school should establish a clear governance structure for data-driven educational tools, starting with leadership approval of their intended educational purpose. School leadership must ensure that LA is used ethically—avoiding punitive or high-stakes applications such as public ranking, penalizing low platform activity, making automatic decisions about progression, or constructing deficit profiles of learners. Best practices in ethical LA stress the importance of transparency, trust, student agency, and educational benefit (Drachsler & Greller, 2016; Slade & Prinsloo, 2013). In school settings, analytics should prompt support, dialogue, and pedagogical adaptation, rather than surveillance or sanctions.

A written local policy should clearly outline: the purpose of each LA system; the data categories involved; access permissions; whether automated inferences are generated; retention periods; responses to alerts; procedures for error correction; external providers involved; and accountability for periodic review. This transparency not only makes data practices visible but also helps prevent individual teachers from using unapproved tools.

Governance should also include regular evaluation. Schools and educational administrations must assess whether analytics tools actually enhance teaching and learning, if teachers find them valuable, whether students understand their purpose, and whether families trust the process. If LA tools cause confusion, increase workload, reinforce inequalities, or fail to deliver pedagogical benefit, their use should be revisited. The aim is not to maximize data collection, but to ensure that the data meaningfully contribute to student learning, equity, and school improvement.

4.3 School Culture

Building a responsible school culture is foundational for effective LA. Before implementing LA, schools should establish clear internal guidelines. Roles and responsibilities must be clearly defined: school leaders should oversee LA tool risk assessment and approval, ensure institutional compliance, clarify educational purposes, organize staff training, and specify necessary safeguards for data privacy and security in collaboration with the Data Protection Officer. ICT coordinators or digital competence coordinators are essential for supporting the technical and pedagogical implementation of LA tools. Teachers should interpret analytics thoughtfully, combining insights with classroom experience to support learning—not to punish or label students.

Parents need clear information about how and why student data are used to be able to support their children's learning, while students should receive age-appropriate explanations, be encouraged to ask questions, understand how their data are processed, and be able to challenge interpretations when needed. Students should not be seen merely as sources of data, but should gradually develop the ability to understand what data are collected, how indicators are interpreted, and how feedback can enhance their own learning. This is essential in informatics education, where understanding data, algorithms, privacy, digital citizenship, AI in education, and responsible technology use are integral parts of the curriculum.

LA should become an opportunity for collective reflection: students, teachers, and parents can discuss what digital traces reveal or conceal, how data might be misinterpreted, and why human judgement is indispensable. A healthy school culture encourages open discussion, acknowledges uncertainty, and values ongoing teacher-student dialogue.

4.4 Professional Development

Successful adoption of LA in schools requires not only infrastructure and resources but also ongoing professional development and robust data literacy among teachers, administrators, and school leadership. Training should be practical and directly connected to everyday classroom scenarios. At a minimum, it should cover four key areas: First, basic data literacy, enabling stakeholders to understand what learning analytics measures (and what it does not), read indicators, identify patterns, recognize limitations, and avoid misinterpretation. Second, pedagogical training so teachers can use analytics for formative feedback and informed instructional decisions. Third, education on ethical and legal considerations—including privacy, data protection, consent, data minimisation, and effective communication with families. Fourth, developing a critical understanding of algorithmic systems, particularly as platforms increasingly use predictive analytics or AI-driven recommendations; this includes recognizing potential errors, biases, and how to interpret predictions. Without comprehensive training, teachers risk overinterpreting weak signals, overlooking bias, depending too much on automated outputs, or avoiding data entirely due to uncertainty or

increased workload. Well-designed professional development ensures staff can integrate LA thoughtfully and confidently into their educational practice.

In summary, responsible school practices are essential for ensuring that LA is used ethically and effectively. By establishing clear governance, supporting ongoing professional development, fostering a collaborative school culture, and prioritizing student agency and privacy, schools can maximize the benefits of LA while protecting the rights and well-being of their communities. Through thoughtful policies and dialogue, schools create a foundation for data-driven approaches that truly enhance teaching, learning, and trust.

References

Drachsler, H., & Greller, W. (2016). Privacy and analytics: It's a DELICATE issue. A checklist for trusted learning analytics. In Proceedings of the Sixth International Conference on Learning Analytics & Knowledge (pp. 89–98). Association for Computing Machinery. https://doi.org/10.1145/2883851.2883893

Slade, S., & Prinsloo, P. (2013). Learning analytics: Ethical issues and dilemmas. American Behavioral Scientist, 57(10), 1510–1529. https://doi.org/10.1177/0002764213479366