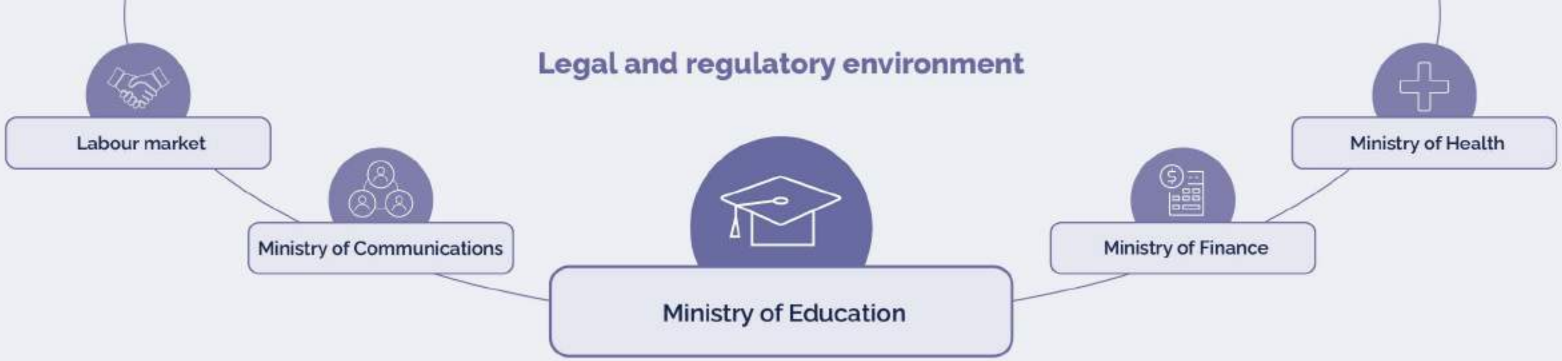
JOB BOARD FOR DATA GOVERNANCE AND MANAGEMENT IN THE EDUCATION SECTOR



Legal and regulatory environment

Labour market

Ministry of Communications

Ministry of Education

Ministry of Finance

Ministry of Health

Please note that these roles and/or titles vary depending on the context.

Macro level

Responsibilities related to the design and management of education data infrastructure and security policies at centralized level and/or a dedicated education data governance team or steering committee

- Chief Information Officer (CIO)
- Chief Data Officer (CDO)
- Chief Information Security Officer (CISO)
- Learning Technologies Specialist (LTS)
- Data Analysts
- Data Privacy and Protection Officer (DPPO)

Meso level

Responsibilities at regional levels of public administration and education management

- Regional IT Specialist
- Regional Data Officer
- Regional Data Privacy and Protection Officer

Micro level

School- and community-level responsibilities needed to responsibly unlock the potential of purposeful data use to improve educational experiences

- School Leaders
- Teachers
- School IT and Cyber Security Officer

BROADBAND COMMISSION FOR SUSTAINABLE DEVELOPMENT
unesco

JOB BOARD FOR DATA GOVERNANCE AND MANAGEMENT IN THE EDUCATION SECTOR

A tool to signpost the baseline roles recommended to ensure accountability, compliance, privacy and security in the use of education data to improve quality and equity in all learning systems

How to use this job board

What is the scope of this tool? This education sector job board represents an ideal baseline of **responsibilities, skills and competencies** that countries should strive to integrate into their education data governance framework and architecture.

- The jobs outlined across micro, meso and macro levels are not derived from a particular country context, but rather exist within an abstracted model of centralized education data governance. Given the diversity of how education systems are structured around the world, the manifestation of the functions, skills and competencies might take different forms. In reality, these jobs may be attributed to more than one individual, or under a different job title in a given context.
- Governance of education data extends beyond the education sector, and responds to broader legal frameworks. This tool acknowledges these links while maintaining focus on the education sector.

What is the intended use of this tool? Each job on the board serves as a representative **signpost** for a set of necessary skills and responsibilities. This signposting supports education data decision-makers to reflect on gaps and strengths within their own education data governance architectures, and to provide a vision for a baseline standard in human terms.

- The job board can be further used to ignite or stimulate discussions among stakeholders at all levels to ensure that data security, compliance, ethics and data protection considerations have been operationalized.
- The tool can be used by governments, education partners, teacher representative organizations and professional bodies, foundations, and not-for-profits and civil society actors, to self-reflect on data governance structures within their own organizations and across the education sector.

What is this tool helping to achieve? The point of departure is the safe management and delivery of education for all children, and the data governance structures, skills and literacies needed to support this goal.

- Using the tool could then bolster the case for increased investments in capacity-strengthening and human resources for data governance, including through the improvement of staff skills and competencies and/or recruitment for key roles. In this way, education authorities move a step closer towards effective, equitable and safe use of data for learning, teaching, and education administration and management.

Where are the jobs, skills and competencies sourced from? There are four types of sources that inspired this job board: (1) international frameworks both directly and indirectly related to data governance, (2) general regional frameworks related to data use, (3) frameworks specific to data in the education sector, and (4) national standards, skills and certification frameworks that support education data governance.

Data governance and identifying the skills needed

1. What do we understand by data governance in the education sector?

There is no universally standardized definition of data governance specifically tailored to the education sector. However, for the purposes of this job board, data governance generally refers to *the establishment and enforcement of policies, procedures, principles, standards and practices to effectively and responsibly manage and monitor data use within educational institutions and across diverse education stakeholders*.

It involves the development of frameworks and strategies to maximize the value, quality, security, privacy, ethics and accessibility of data while ensuring accountability for compliance with relevant laws, regulations and ethical considerations. The definition also takes into account notions related to data subject rights; protecting the privacy of individuals; data security and incident response; data protection by design and default; lawfulness, fairness and transparency; accountability and data standards; benchmarking and auditing; and data protection impact assessments (DPIAs).

2. Why does data governance in the education sector matter?

Effective data governance in the education supports:

2.1. The protection of the rights of learners, teachers and the education workforce at every level

First and foremost, education data governance should ensure that there are clear sector-specific standards for the safe and transparent use of all learner-level data, that are explainable to all education stakeholders, from learners to education technology (EdTech) providers.

Likewise, education data governance should regularly ensure that evolving technologies used in education systems **meet regulatory requirements**, notably by safeguarding the rights of all learners, teachers and the education workforce by promoting **data security, privacy, transparency and fairness** in data use and by mitigating all risks related to data misuse.

2.2. Education system efficiency, which is needed to expand access to educational opportunities, ensure quality education and improve learning outcomes, particularly for underserved population groups

Data governance should ensure that all technologies interacting with learner-level data, and in particular those provided by industry vendors, are optimized to generate an education data architecture supporting safe and compliant **data collection, analysis and integration** across different education planning, management, reporting and delivery functions.

The resulting data outputs can support decision-makers to develop **evidence-based strategies** for improving learning outcomes, invest in targeted actions to serve marginalized learners, and improve system management efficiency and functioning.

2.3. The integrity and usability of education data used to support decision-making

Data governance should ensure the **quality, reliability, accuracy and trustworthiness** of all data used in education decision-making. Such guardrails are vital in the context of increasingly complex and interoperable data management platforms, and in the face of new, powerful technologies which can treat large volumes of data from different sources, such as those powered by generative artificial intelligence (AI).

Usability of education data should be maintained through all governance levels, with an efficient data architecture that allows for collaboration across functional areas to **counter data silos** and **promote interoperable data management**. Such interoperable systems must be regularly audited and assessed for compliance with government standards that protect the user, while providing a streamlined and standardized experience to improve data usability for all learners and the education workforce.

3. Responsibilities and skills identified within the job board

This job board represents an ideal baseline of responsibilities, skills and competencies that countries should strive to integrate into their education sector data governance framework and architecture. The jobs outlined across **micro**, **meso** and **macro** levels are not derived from a particular country context, but rather exist within an abstracted model of centralized education data governance.

Each job on the board serves as a signpost for a set of necessary skills and responsibilities, which, in reality, may be attributed to more than one individual or come under a different job title in a given context. This signposting supports education data decision-makers to reflect on gaps and strengths within their own education data governance architectures, and to provide a vision for a baseline standard in human terms.

Macro level: Responsibilities related to the design and management of data infrastructure and security policies at centralized level and/or a dedicated data governance team or steering committee

Meso level: Responsibilities at regional levels of public administration and education management

Titles: Actors at macro and meso levels often carry distinct and complementary job titles and responsibilities related to data management and security, compliance with regulatory requirements, and technology procurement. Responsibilities can be formalized within designated roles (e.g. Chief Information Officer [CIO] and Chief Information Security Officer [CISO] covering the oversight of technology infrastructures and data security policies) or connected to stewardship within a dedicated data governance steering committee.

Architecture: A well-designed data governance architecture would effectively include a data governance team or steering committee that acts as the overarching governing body. Senior management work together to create common definitions and standards supporting a shared understanding of data governance across the education sector (or public sector), as well as standards and policies for governing data and enforcing procedures under the custodianship of data stewards (i.e. connected to specific job roles). These roles may be situated within a ministry or institutional body charged with public sector digital or information technology (IT) policy, and/or specifically within the education sector.

Competencies: These senior-level jobs require specific IT and technical skills and literacies to oversee and engage with the latest technologies – including cloud-to-edge technologies and the use of generative AI – and the latest data governance practices both across sectors and within education specifically.

Micro level: School-level and community-level responsibilities needed to responsibly unlock the potential of purposeful data use to improveeducational experiences

Resource dependency: At micro level, while there may be an appointed IT person charged with technical trouble shooting, IT staff support and cybersecurity for the school community, it is important to note that this may not be feasible in low-resource contexts where governments are already struggling with school maintenance costs and paying teacher salaries. Specific requirements and skillsets at this level will also depend on the size and complexity of the school's IT infrastructure and the resources available to recruit a dedicated IT officer.

Data ethics and rights: Across all cases at the school level, skills and competencies for data governance directly include the active protection of learners', teachers' and families' data rights, including informed consent, protecting access to data, and opting out). To this extent, data governance at school level is often expressed in terms of the data literacy now needed by school leaders, teachers, learners and community members to access (or opt out of) tech-enabled learning tools and learning management systems, or to participate in large-scale data collection and learning assessment through dedicated apps and platforms.

4. References: Governance frameworks, skills accreditation and certification programmes as a support for strengthening governance practices in the education sector

The level of involvement of actors in education data governance at macro, meso or micro levels depends on the public sector management structure, and the policies in place in individual countries and regions. Given the diversity in how education systems are structured around the world, the manifestation of the functions, skills and competencies might take different forms. Existing national and international skills frameworks, standards, accreditation programmes and professional certifications can provide valuable guidance, knowledge and skills related to data governance practices, and in identifying the types of roles and skills appropriate to different contexts.

To this end, the following international, regional and national data management and governance frameworks could be of use:

International frameworks directly and indirectly related to data governance

Click for links

DAMA-DMBOK	The Data Management Body of Knowledge (DAMA-DMBOK) provides a comprehensive framework for data management, including data governance. It defines a set of knowledge areas, such as data governance and stewardship, and outlines the skills, roles and responsibilities associated with each area.
COBIT	Control Objectives for Information and Related Technologies (COBIT) is a framework developed by ISACA that provides guidance on IT governance and control. It includes domains related to data management, and can help in understanding the governance of data within the broader IT context.
ITIL	The IT Infrastructure Library (ITIL) is a widely adopted framework for IT service management. Although it does not specifically address data governance, it provides a structured approach to managing IT services, including aspects which are relevant to data governance, such as data security, incident management and service delivery.
SFIA	The Skills Framework for the Information Age (SFIA) is a globally recognized skills framework that covers a broad range of IT and digital skills. It can be useful in identifying and understanding the skills required for data governance roles, such as data stewards, data managers, or data governance officers.
ICRM	The Institute of Certified Records Managers (ICRM) offers certifications related to records and information management. While data governance and records management are not identical, there is an overlap in terms of data governance's focus on data quality, integrity and compliance, which can benefit from an understanding of records management principles.
ISO/IEC 38500	This international standard, titled "Corporate governance of information technology", provides guidelines for the effective governance of IT, including data governance. While it focuses on IT governance as a whole, it can offer insights into the governance aspects relevant to data.
CIPP	The Certified Information Privacy Professional (CIPP) certification offered by the International Association of Privacy Professionals (IAPP) is globally recognized and focuses on privacy laws, regulations and best practices, including data governance considerations.

ISO/IEC 27001	This international standard provides a comprehensive framework for establishing, implementing, maintaining and continually improving an information security management system (ISMS), which encompasses data governance aspects.
CDMP	The Certified Data Management Professional (CDMP) certification offered by DAMA covers a wide range of data management disciplines, including data governance, data quality, data architecture and more, providing a holistic approach to managing enterprise data.
ISACA	The Information Systems Audit and Control Association (ISACA) provides globally recognized certifications like Certified in the Governance of Enterprise IT (CGEIT) and Certified Information Systems Auditor (CISA) that cover various aspects of data governance, ensuring compliance with regulatory frameworks and best practices.

Regional frameworks

GDPR	The European Union General Data Protection Regulation (GDPR) is a comprehensive data protection and privacy regulation that applies to all European Union member states and sets out requirements for data controllers and processors regarding the collection, storage, processing and transfer of personal data. It establishes principles for data governance, such as transparency, accountability and individual rights.
ESCO	European Skills, Competences, Qualifications and Occupations (ESCO) is a European multilingual classification of skills, competences, qualifications and occupations.
DigComp 2.2 Framework	The 2022 version of the European Union's Digital Competence Framework for Citizens, with five dimensions that include data-related competencies.
CIPP/E	The Certified Information Privacy Professional/Europe (CIPP/E) credential, offered by the IAPP, focuses on European data protection laws and practices. Understanding privacy regulations and compliance is crucial for data governance, and this certification provides knowledge in that area.

Education sector-specific frameworks

UNESCO	Global Media and Information Literacy Assessment Framework: Country Readiness and Competencies.
GESS	Version 1.0 of the Global Education Security Standard (GESS), the first ever international education sector-specific data security standard, reflects the combined work and outputs of a multinational team dedicated to improving the cyber safety of the education sector.
Standards for Education Leaders	The International Society for Technology in Education (ISTE) has developed this broad set of competencies that support the skills defined in this job board, especially at the school system and building level.

SDPC	The Student Data Privacy Consortium (SDPC) is a collaborative effort among education service providers, states, districts and other stakeholders focused on ensuring the privacy and security of student data. They provide guidelines, resources and a framework to help educational institutions develop robust data governance practices.
NICE Framework	The Workforce Framework for Cybersecurity (NICE Framework) categorizes and describes various cybersecurity roles, knowledge areas and skill sets. It serves as a common language for describing and organizing cybersecurity work roles, and assists in identifying the skills and competencies required for specific positions within the education sector. The NICE Framework provides a structured approach to defining cybersecurity roles and aligning them with the needs of educational institutions.

Country example of national standards, skills and certification frameworks (United States of America)

NIST	The National Institute for Standards and Technology (NIST) provides resources on computer, cyber- and information security and privacy.
Essential Skills of the Chief Technology Officer	From the Consortium for School Networking (CoSN), this framework provides a list of competencies as part of a broader certification framework, the Certified Education Technology Leader.
AASA National Superintendent Certification Program	A training programme.
New England Association of Schools and Colleges framework	An accreditation framework.
Teacher Educator Technology Competencies Program	Prepares teacher and school leader candidates (pre-service) and current staff (in-service).
American Association of Colleges for Teacher Education	A comprehensive analysis of the most recent teacher preparation data.

There are common aspects of job functions, responsibilities and required skills cited across all these frameworks to ensure that education authorities (and individuals) can leverage the latest data management, security and governance practices, and ensure efficient and responsible data management within the education sector that is oriented towards protecting and benefiting learners. These frameworks have served as the sources for the job board in this document.

MACRO LEVEL

<table>
<tr><th>Job functions</th><th>Skills and competencies</th></tr>
<tr><td colspan="2">

Chief Information Officer, education sector

The CIO in the education sector is a senior executive responsible for overseeing and managing IT infrastructure across education management authorities at national, federal and/or decentralized management levels, as well as the IT supporting tech-enabled learning at pre-primary, primary and secondary levels. This senior management role supports the definition and approval of data and IT policies, strategies and annual budgets related to all data-related infrastructures, services and products, including integration with national learning goals and strategies. They ensure that the IT infrastructure is reliable, secure and capable of supporting the sector's technological and data requirements.

The CIO also supports the management and data governance of the dedicated Education Management Information System (EMIS). To facilitate strategic planning and collective decision-making, the CIO often serves as the chair of the Education Data Governance Steering Committee, working closely with other members such as the CISO, Chief Data Officer (CDO), Digital Learning Strategists, Analysts and Compliance Officers.

Key responsibilities and expected competencies and skills of a CIO in the education sector are outlined below:

</td></tr>
<tr><td>

Strategic planning: The CIO collaborates with national education leaders, including ministers and vice-ministers and principal education decision-makers and administrators at different management and governance levels, to develop a strategic technology plan aligned with the sector's goals and objectives (including integration with broader digital society and transformation policies). They identify technological needs at every level, assess capacity needs and potential risks, and formulate strategies to address them.

</td><td>

- **Strategic thinking:** Strong strategic thinking skills to assess the sector's current technological landscape, identify future opportunities and challenges, and develop a long-term vision for technology integration in support of educational goals and targets.
- **Leadership and management:** Strong ability to guide and inspire IT teams at different levels and build a cohesive IT department, setting clear objectives, delegating responsibilities, and fostering a culture of innovation and continuous improvement.
- **Data analysis and decision-making:** Familiarity with complex data sets and leveraging analytics to interpret macro-level trends, inform strategic planning and measure the impact of technology initiatives.

</td></tr>
</table>

Technology infrastructure: The CIO oversees the design, implementation and maintenance of the sector's comprehensive IT infrastructure, including: • design and maintenance of EMIS hardware and software architectures (including databases) • integration of emerging AI and machine learning (ML) with sector education goals, objectives and emerging opportunities, including the integration of AI- and ML-powered data management solutions and automated data quality measurement tools to support education data governance • oversight of appropriate telecommunications systems, networks, servers, hardware and software	• **Technological expertise:** Strong understanding of the latest technologies (cloud-to-edge, ML, generative AI etc.), data trends and innovations relevant to education data management and services. • **Software expertise:** Well-versed in educational software, learning management systems, data analytics tools, cybersecurity practices, and emerging technologies such as AI and virtual reality. • **Experience in EMIS:** Knowledge of management information systems (MIS), computer information systems (CIS), IT management and project management. • **Pedagogical insights:** Knowledge of emerging trends in learning technologies, and ability to work with learning technology specialists. • **Change management:** Expertise in change management around technology implementation, including foresight, assessing readiness, managing resistance, and effectively communicating with and supporting stakeholders through transitions. • **Adaptability and learning agility:** Strong capacity to stay updated on emerging trends, new technologies and best practices.
Data management, compliance and cybersecurity: The CIO works with the CISO and Data Officers to develop IT standards and procedures for managing and safeguarding sensitive data through robust security measures and privacy compliance. This includes compliance with relevant laws, regulations and data protection requirements.	• **Capacity to analyse operations, identify risks and opportunities:** Includes awareness of national legal standards for data privacy and security and experience in ensuring compliance with rules and regulations and administrative processes, and excellent understanding of technology management and monitoring.
Budgeting and resource allocation: The CIO has overall responsibility for managing the IT budget, ensuring that financial resources are allocated and managed appropriately, and regularly reviewed to support the sector's technology needs. They assess technology investments, support negotiations around contracts with vendors, and identify cost-effective solutions to optimize the use of available funds.	• **Strong financial management skills:** Skills for developing and managing IT budgets effectively, including the ability to use and analyse cost-benefit ratios.
Collaboration and stakeholder management: The CIO collaborates with various members of the IT and data teams and education stakeholders, including high-level decision-makers and administrators and external partners. They build relationships with technology providers and industry experts to stay updated on emerging trends and advancements in educational technology.	• **Strong vendor and stakeholder management:** Including skills to engage with external vendors, technology providers and industry experts, evaluate vendor offers, and negotiate contracts. • **Team management, collaboration and communication:** Experience in leading, supervising, managing and motivating IT staff and teams, and ability to establish good working relationships with educational leaders, teachers, administrators, and external and internal partners, including with CIOs from other sectors of national government.

Chief Information Security Officer, education sector

The CISO sets the lighthouse standards for cybersecurity leadership and guidance for the entire education sector. The CISO is charged with protecting the sector's data and information assets, ensuring compliance with privacy regulations, national cybersecurity policy, standards and legislation, fostering a culture of security awareness to mitigate cyber threats, and maintaining a secure and trusted teaching and learning environment. They do this by developing, implementing and maintaining a cybersecurity strategy across the education sector that ensures confidentiality, integrity and availability of all data assets, as well as protecting them from unauthorized access, data breaches and cyber threats. In short, the CISO's role (in collaboration with the CIO) is crucial in safeguarding sensitive staff, student and teacher data, and mitigating security risks.

Key responsibilities and expected competencies and skills of a CISO, including a combination of technical, managerial and strategic skills, are outlined below:

Information security strategy: The CISO develops and implements an overarching data security strategy for the education sector that covers EMIS systems, the deployment of complex databases and analytic platforms, use of cloud-to-edge technologies, learning management systems and generative AI. This includes defining security objectives, establishing policies, guidelines and procedures, and identifying security controls to protect data and information assets. To do their job, the CISO collaborates with internal stakeholders, such as IT teams and the CDO (see below), senior leadership, and legal or compliance departments, to design and implement the security strategy, and regularly reviews and updates it to ensure its relevance in the face of changing technologies and emerging threats. They also establish partnerships with external entities, such as compliance agencies, industry associations and information-sharing forums, to enhance security capabilities and respond to security challenges effectively.	• **Knowledge of relevant laws, regulations and standards in the education sector:** Knowledge of data protection regulations (e.g. GDPR), industry frameworks (e.g. ISO 27001), and any specific compliance requirements for educational institutions. • **Strong leadership, team cooperation and communication skills:** To articulate complex security concepts in a clear and concise manner, and effectively engage with stakeholders including decision-makers and education staff at all levels, about security best practices and collaborating with cross-sector departments to implement security initiatives.
Security architecture and infrastructure: The CISO collaborates with IT teams to design, implement and update secure data-sharing systems, networks and infrastructure. They ensure that security controls, such as firewalls, intrusion detection systems and encryption mechanisms, are effectively deployed to protect sensitive data. They work with stakeholders to establish data access controls and data stewardship practices. They also monitor security-related legal and regulatory developments to adapt policies and procedures accordingly.	• **Security architecture expertise:** A strong understanding of information security principles, practices and technologies, including knowledge of the technical aspects of network security, encryption, vulnerability management, access controls, incident response and regulatory compliance.

Risk assessments and incident monitoring: The CISO stays informed about the latest threats and vulnerabilities posed by AI, ML, and cloud and edge technologies, by monitoring threat intelligence sources. They perform periodic security audits and assessments to evaluate the effectiveness of security controls, identify vulnerabilities, recommend improvements and oversee risk mitigation measures. The CISO also investigate potential security breaches or incidents and restores normal operations. This includes the use of intrusion detection systems, log analysis, and security information and event management (SIEM) tools. They also develop incident response plans to handle security incidents effectively, and conduct post-incident analysis to learn from lessons and improve incident response procedures.	• **Risk management:** The ability to assess and manage risks, including identifying potential threats, evaluating their potential impact and implementing appropriate controls to mitigate those risks. A CISO should be skilled in risk assessment methodologies and have experience in developing risk management strategies. • **Continuous learning:** The cybersecurity landscape is ever evolving, so a CISO must stay updated on the latest threats, vulnerabilities and security technologies. This involves participating in industry conferences, attending training sessions and engaging with professional networks to continually enhance knowledge and skills. • **Detect and respond to security incidents:** A solid understanding of incident response processes, including containment, investigation and recovery. Knowledge of digital forensics and incident handling techniques is also valuable for conducting post-incident analysis.
Staff awareness and training around security issues: The CISO promotes security awareness among institutional staff at different management levels, and among school leaders, teachers and students. They develop and deliver training programmes to educate individuals on best security practices, such as password management, phishing awareness and data protection.	• **Training and education expertise:** Solid understanding of adult learning principles and instructional design methodologies to develop and deliver effective security training programmes tailored to different roles and levels across the education sector, including engaging and interactive training materials for presentations, videos, quizzes and simulations.
Vendor and third-party risk management: The CISO works with data teams and legal and compliance departments to assess the security posture of third-party vendors and service providers. They establish guidelines for vendor selection, conduct security assessments and monitor the ongoing security practices of external entities that have access to the sector's data or systems.	• **Vendor management skills:** To assess the security posture of vendors, establish security requirements in contracts, and conduct regular audits or assessments to ensure compliance.

Chief Data Officer, education sector

The CDO works with the CIO in overseeing the sector's education data management. This might include national data covering learners, teachers and schools, as well as academic data, financial data, research data and operational data. It also covers data made available and shared through cross-national dataflows. The CDO works closely with stakeholders at all levels to identify data needs and ensure data quality, integrity and usability. The CDO also collaborates with cross-sector departments, such as planning and finance, to implement strategic data management practices and promote data-driven decision-making.

Principle responsibilities of the CDO are outlined below, although these bleed into other areas such as data governance and compliance.

Data strategy and planning: Develops and implements a comprehensive education data strategy aligned with the sector's strategic goals and security needs. This involves:

- identifying specific national, regional and international data needs, e.g. related to monitoring and reporting agreements around regional development frameworks and the Sustainable Development Goals (SDGs), or participation in international learning assessments such as the Programme for International Student Assessment (PISA)
- establishing data management policies and procedures
- generating data definitions, classifications and standards
- pushing for convergence in awareness around data across institutional functions at different governance levels
- providing support to application of data policies and governance frameworks, including around big data and cross-border data flows

- **Data management and analysis:** Strong understanding of data management principles, data modelling and data analysis techniques. Proficiency in data management tools, databases and data visualization tools. Knowledge of statistical analysis and data-mining methods.
- **Strategic thinking:** Ability to align data initiatives with the organization's strategic goals and objectives. Develop long-term data strategies that support educational outcomes and institutional effectiveness. Understand the value and potential of data-driven decision-making.

Data integration, sharing and effective use for education decision-making purposes: Facilitates cross-functional and cross-department collaboration to ensure optimization of technologies, data management systems, and tools for data collection, integration, validation and storage. This includes the ability to exploit interoperability within cloud-to-edge technologies and AI to integrate and harmonize data from various sources and formats within cloud and edge environments.

Data standards: The CDO further supports the definition of data standards and guidelines to ensure data quality and consistency in the context of complex data interfaces and interoperability, and works with the CIO and CISO in developing policies for data governance, stewardship, ownership and access, including sharing rights and retention.

- **Expertise in developing and implementing data policies:** Deep understanding of data management and governance practices, and data strategy development. Ability to establish policies, procedures and guidelines to ensure consistent data quality, formats, security, privacy and compliance within the sector.
- **Communication and collaboration:** Ability to collaborate with different departments and build strong data management relationships with diverse stakeholders.
- **Leadership and team management:** Strong leadership skills and ability to build and manage a high-performing data management team. Provide direction, mentorship and support to staff members.
- **Change management:** Ability to navigate organizational change related to data management initiatives, drive cultural transformation towards a data-driven culture, help stakeholders understand the benefits of data-driven decision-making, and foster data literacy within the organization.

Data Privacy and Protection Officer

The Data Privacy and Protection Officer (DPPO) supports data governance by bringing their expertise to management so that compliance with data practices can be ensured. Their main responsibility is to be the "orchestra conductor" of the management of personal data in the organization, and to assist the organization to monitor compliance with the provisions relating to the protection of personal data. However (at least in Europe), according to Article 29 of the Guidelines on Data Protection Officers published by the EDPB, "DPOs (Data Protection Officers) are not personally responsible in case of non-compliance with the GDPR. The GDPR makes it clear that it is the controller or the processor who is required to ensure and to be able to demonstrate that the processing is performed in accordance with its provisions (Article 24(1)). Data protection compliance is the responsibility of the controller or the processor."

Data privacy and compliance: The DPPO assists the sector in monitoring compliance with data protection regulations (e.g. GDPR in Europe) and other relevant national privacy laws. Their main responsibilities include:

- developing and implementing data privacy policies and procedures
- assisting the organization to monitor compliance with national data protection laws and collaborating with internal teams, such as IT, legal, human resources and business units, to align data governance practices with privacy requirements
- implementing data privacy training and awareness programmes
- providing advice on privacy impact assessment and monitoring its performance [1]
- participating, in particular with the CISO, in the personal data breach management and incident management
- monitoring and auditing data practices
- cooperating with the supervisory authority and acting "as the contact point on issues relating to processing […] and to consult, where appropriate, with regard to any other matter"[2]

The role requires a combination of technical knowledge, legal understanding and interpersonal skills, including knowledge of:

- **Data protection laws:** A solid understanding of relevant data protection and privacy laws, such as the GDPR in the European Union and the Family Educational Rights and Privacy Act (FERPA) in the United States of America.
- **Education regulations:** Familiarity with specific data regulations that apply to the education sector, such as the Children's Online Privacy Protection Act (COPPA) or the Individuals with Disabilities Education Act (IDEA).
- **Privacy by design principles:** Knowledge of privacy by design principles and the ability to embed privacy safeguards into systems, processes and applications right from the design phase.
- **Privacy impact assessments (PIAs):** Ability to provide advice as regards the privacy impact assessments to identify potential risks and evaluate the impact of data processing activities on individuals' privacy rights.
- **Risk management:** Skill in assessing risks related to data privacy and protection, and developing strategies to mitigate those risks effectively.
- **Information security:** Understanding of information security practices, including encryption, access controls, authentication, and secure data storage and transfer methods.
- **Continuous learning:** A commitment to staying updated with the evolving landscape of data privacy and protection laws, regulations and best practices through ongoing professional development and networking.

[1] According to Article 35(1) of the GDPR, it is the task of the controller, not the DPPO, to carry out, when necessary, a data protection impact assessment. Article 39(1) (c) tasks the DPPO with the duty to "provide advice where requested as regards the [DPIA] and monitor its performance."

[2] According to Article 39(1)(d) and (e) of the GDPR, the DPPO should "cooperate with the supervisory authority" and "act as a contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter."

Learning Technologies Specialist

The Learning Technologies Specialist (LTS) works with the CIO in designing national learning management systems (LMSs), digital learning platforms (DLPs) and digital content repositories, as well as integrating and implementing other technology tools and resources to enhance the teaching and learning experiences.

Technology integration with teaching and learning processes: The LTS provides technical and pedagogical advice and support to the senior management team in leveraging technologies to support instructional practice and create innovative learning environments to improve education outcomes.
To this end, the LTS collaborates with the CIO and other LTSs and instructional designers to identify and implement technology tools, resources and platforms that enhance teaching methods, facilitate online learning, and promote digital literacy among students.

- **Education insights:** An understanding of the unique IT infrastructure needs and challenges of the education sector, including educational trends, pedagogy, and the evolving demands of students, teachers and administrators.
- **Communication and collaboration:** Excellent communication skills to understand technological needs and effectively communicate complex technological concepts to all stakeholders. Experience in translating teaching and data insights into actionable technology recommendations. Ability to collaborate with different departments and build strong relationships.

Data Analysts

Data Analysts facilitate and enable data-driven decision-making, as well as generating meaningful insights on learning and teaching, by extracting data from databases and using data to identify trends, patterns and correlations in educational data.

Identifying trends and insights: The Data Analyst works with the CDO and other data analysts and researchers to:

- manage stakeholder requirements for management and reporting data across education departments and governance levels
- analyse and collate critical data related to learning and provide actionable insights to inform strategic planning, policy development and monitoring requirements
- develop and maintain procedures for monitoring database activity and optimizing databases to forecast education needs and establish trends

- **Database proficiency:** Understanding of education databases (enrolments, learning assessment results etc.), data storage, mining, retrieval, integration and governance practices. This includes proficiency in managing and organizing data in cloud- and edge-based environments, and ML-based data quality tools.
- **Technical skills:** Strong skills in data manipulation, data cleansing and data integration using tools such as SQL, Python, R or other programming languages commonly used in data analytics. Familiarity with data analytics platforms and tools for data visualization and reporting like Tableau, Power BI or Excel.
- **Data pattern analysis and interpretation:** Proficiency in statistical methods and data visualization tools. Includes predictive analytics to identify trends, patterns and correlations in educational data.
- **Education domain knowledge:** Knowledge of the education sector, including understanding of educational data, performance metrics and the factors that impact educational outcomes. Familiarity with academic data, student data, assessment data and institutional data in the context of the education sector.
- **Continuous learning and adaptability:** Keeping up with the latest trends, tools and methodologies in data analytics. Being adaptable to new technologies and evolving data practices in the education sector. Willingness to learn and explore new techniques to improve data analysis and insights generation.

MESO LEVEL

Job functions	Skills and competencies

Regional Data Officer

A Regional Data Officer is responsible for managing and analysing data within a decentralized regional education office. They are charged with ensuring data quality and integrity while promoting secure data governance practices. They also collaborate with central management and school-level stakeholders to identify data needs, develop data-collection methods, and design reporting frameworks supporting school improvement and teacher professional development practices. As such, they play a crucial role in generating insights and providing actionable recommendations to support decision-making at the regional and national levels.

Job functions	Skills and competencies
The Regional Data Officer: • oversees the collection, storage and management of education data, and overall quality assurance for data submitted by the educational levels and institutions under their supervision • contributes to the implementation of policies and guidelines related to education data governance at the regional or provincial level, including in relation to the use of cloud-to-edge technologies, ML tools and generative AI	• **Strong project management skills and familiarity with data management and governance:** To effectively plan, implement and monitor data management and governance initiatives at decentralized level. Familiarity with data management systems and emerging technologies requiring evolved practices in data governance. Capacity to address challenges and make informed decisions related to data governance and privacy issues.

Regional IT Specialist

The Regional IT Specialist is responsible for overseeing and managing the IT infrastructure for education management and tech-enabled learning in regional/district-level education offices, education authorities and schools, ensuring the smooth operation of technology systems, including hardware, software and network infrastructure. They address technical issues, provide user support, and implement IT policies and procedures, including data security policies.

Job functions	Skills and competencies
The Regional Technology Specialist: • provides guidance and support to education institutions and schools in implementing digital learning and data-collection initiatives • supports the installation, maintenance and security of computer systems and networks • troubleshoots and resolves technical LMS and cloud-to-edge technology issues	• **Excellent knowledge of latest technologies supporting data management and LMSs:** Includes familiarity with the benefits and limitations of cloud-based solutions and cloud computing concepts including cloud storage, virtualization and cloud service models. Understanding of edge computing principles and technologies relating to processing and analysing data closer to the source (at the edge). • **Familiarity with LMSs and interfaces:** Appropriate knowledge of DLPs and tools in order to provide technical support teachers in integrating technology in the classroom.

- provides training/guidance for education staff and teachers on technology integration
- engages with relevant stakeholders, such as teachers, principals, parents and students, to understand their IT needs, address concerns and gather feedback

- **Problem solving and troubleshooting:** Capacity to identify and resolve technical issues related to connectivity, system failures or data inconsistencies.
- **Continuous learning:** A mindset of continuous learning to keep up with advancements in cloud-to-edge technologies, emerging technology trends and best practices.
- **Communication and collaboration:** Excellent communication, interpersonal and collaboration skills to engage with stakeholders at decentralized administration and school level, facilitate cooperation, and convey complex concepts to non-technical audiences.

Regional Data Analytics Officer

The Regional Data Analytics Officer works with the Regional Data Officer to generate actionable insights for decision-making. They work with other analysts to analyse large data sets, employ statistical techniques and use data visualization tools to identify patterns, trends and opportunities. They also collaborate with other regional stakeholders to understand organizational and institutional objectives, develop analytical models, and provide strategic recommendations based on data-driven insights.

The Regional Data Analytics Officer:

- implements mechanisms to ensure the accuracy, reliability and consistency of education data
- analyses education data to generate insights and reports that inform decision-making processes

- **Proficiency in managing and organizing databases, including in cloud-based and edge-based environments:** Including skills in data storage, data retrieval, data integration and data governance practices.
- **Proficiency in using data analytics tools and techniques to extract insights and value from the collected data:** Including skills in data visualization, statistical analysis, ML and predictive modelling.

Regional Data Privacy and Protection Officer

The Regional Data Privacy and Protection Officer assists the organization to monitor compliance with data privacy laws and regulations within a specific geographical region or area of an organization. When needed, they provide advice on PIAs, audits and risk analyses to identify vulnerabilities and mitigate potential data breaches. Additionally, they provide guidance and training to decentralized education staff and schools on data privacy best practices, and act as a point of contact for privacy-related concerns within the region.

The Regional Data Privacy and Protection Officer:

- assists the sector in monitoring compliance with data protection and privacy laws, regulations and policies within the education sector
- identifies and addresses potential risks related to education data governance, including data breaches, privacy violations and unauthorized access
- provides training and support to education staff on data governance practices, data protection and privacy regulations

- **Legal and regulatory knowledge:** Understanding of relevant data protection and privacy laws, regulations and policies within the education sector.
- **Data security:** Understanding of information technologies and data security, including knowledge of encryption techniques, access controls, data privacy regulations and best practices for securing data in cloud-to-edge environments.
- **Ethical considerations:** Awareness of ethical considerations and a commitment to upholding data privacy, confidentiality and security.

MICRO LEVEL

School IT and Cybersecurity Officer

The responsibilities and skills of a School IT and Cybersecurity Officer can vary depending on the resources available to the institution and specific requirements of the post. Generally speaking, their responsibilities revolve around maintaining and securing the school's technology infrastructure, advising staff on how to ensure data privacy and protection, and supporting the efficient use of technology for educational purposes. Some common responsibilities and skills associated with this role include:

Job functions

- **Network and systems administration:** Managing the school's network infrastructure, including servers, routers, switches and wireless access points.
- **Security infrastructure management:** Implementing and maintaining security measures such as firewalls, intrusion detection systems and antivirus software.
- **Data privacy and protection:** Ensuring compliance with data protection regulations and establishing protocols to safeguard student and staff information.
- **Incident response:** Developing and implementing strategies to respond to and mitigate cybersecurity incidents, such as malware infections or data breaches.
- **User support and training:** Assisting staff and students with technology-related issues, providing training on best practices for online safety and cybersecurity.
- **Risk assessment and management:** Identifying potential vulnerabilities, conducting risk assessments and implementing appropriate controls to mitigate risks.
- **Security awareness programmes:** Organizing and conducting initiatives to raise awareness about cybersecurity among staff, students and parents.

Skills and competencies

- Strong knowledge of computer networks, operating systems and network protocols.
- Proficiency in network and system administration, including configuration and troubleshooting.
- Deep understanding of cybersecurity principles, best practices and industry standards, and knowledge of data protection regulations and compliance requirements (e.g. GDPR, COPPA).
- Experience with security tools and technologies such as firewalls, antivirus software, intrusion detection systems and encryption methods.
- Familiarity with risk assessment methodologies, and the ability to identify and prioritize potential risks.
- Excellent problem solving and analytical skills to respond effectively to cybersecurity incidents.
- Effective communication skills to educate and train users on cybersecurity practices and work collaboratively with diverse stakeholders, including administrators, teachers, students and external vendors.
- Continuous learning and keeping up to date with the latest cybersecurity trends and threats.

School Leaders

- **Assessing data quality:** School leaders need to understand how to assess the quality and reliability of the data they use (through assessments and engagement in digital environments) as part of their management. They should be able to critically evaluate education data, tools and research, and other sources to ensure data validity and make informed decisions, not only about school management and teacher instruction, but also about privacy, age-appropriateness, legal compliance, and procurement of digital tools and services. School leaders need to critically assess the added value of integrating new data-fueled digital tools into school communities, with particular consideration for its wider impact on school well-being and the responsible management of third-party data ownership.

- **Awareness of data governance architecture and legal compliance:** School leaders need to be aware of the main principles of data governance and ownership to inform and protect their teachers' and learners' privacy and human rights. School leaders should be able to identify both the positive and negative implications of the use of data, and weigh the benefits and risks before allowing third parties to process personal data from their school community. They should know the legal and policy frameworks applicable to their school contexts and how these implicate rights to informed consent, who has access to student data, whom it is safe to share data with, how access is monitored, how long data are retained, and how data can be deleted.

- **Understanding the impact of data use on humans and human rights:** School leaders should know how a given digital system addresses the different social objectives of education, and how data profiling can influence societal decision-making. School leaders should be able to consider the impact of data use on the school community, including carefully considering parents' access to student and teacher data. School leaders should be able to article how a specific use of data can benefit all students, independent of their cognitive, cultural, economic or physical differences. School leaders should be able to consider the impact of data use (grading, taking attendance, monitoring student behaviour, using learning analytics, generating automated feedback and assessment, professional development, and school progress-monitoring) on the development of teacher and student workload, social engagement, self-efficiency, self-image, mindset, and self-regulation skills.

- **Ethical data-driven decision-making:** School leaders should also be able to interpret and analyse basic data gathered through classroom practice, LMSs, national- and school-based learning assessments, and other types of large-scale, tech-based data collection, to inform strategic school management decisions and other types of decision-making. Capacities are needed to responsibly leverage data outputs and insights to assess student performance, identify areas for school improvement, and allocate resources effectively. Across use cases, teachers should consider potential analytic biases caused by various data-related factors, including algorithms, censorship or limitations in their own data literacies.

- **Communicating data insights:** School leaders need strong communication skills to effectively communicate data insights to various local stakeholders, including teachers, parents, governing bodies, and regional education authorities and school inspectorates. They should be able to present data in meaningful and accessible formats to facilitate understanding and support decision-making. They should be able to communicate how learner data was collected, used, stored and/or transferred in order to produce these insights.

- **Environmental impact:** School leaders should understand the environmental impact of everyday digital practices that rely on data transfer, which produces carbon emissions from devices, data centres and network infrastructures. In particular, they should understand the energy intensive processes that power digital learning environments which employ AI to operate, and this understanding should influence their procurement processes of certain tools and the time which they recommend teachers and students spend interacting with them.

Teachers

- **Ethical data-informed instruction:** Teachers should be aware of the various forms of personal data used in education and training. Teachers should be able to collect, analyse and interpret student data to inform their instructional practices. Teachers should be able to interpret the data and evidence available in order to better understand individual learners' needs for support. This includes through classroom-based assessments, manual or tech-based tracking of student progress, identifying learning gaps, and adjusting teaching strategies accordingly to meet individual student needs. Across use cases, teachers should consider potential analytic biases caused by various data-related factors, including algorithms, censorship or limitations in their own data literacies.

- **Understanding the impact of data use on humans and human rights:** Teachers should know how a given digital system addresses the different social objectives of education and how data profiling can influence societal decision-making. Teachers should be able to consider the impact of data use on the student community. Teachers should be able to explain how a specific use of data can benefit all students, independent of their cognitive, cultural, economic or physical differences. Teachers should be able to consider the impact of data use (learning analytics, automated feedback and assessment, and progress monitoring) on social engagement and the development of students' self-efficiency, self-image, mindset, and self-regulation skills.

- **Assessing data quality:** Teachers need to understand how to assess the quality and reliability of data they use (through assessments and engagement in digital environments) as part of their teaching. They should be able to critically evaluate education data, educational tools and research, and other sources to ensure data validity and make informed decisions, not only about instruction, but also about privacy, age-appropriateness, and legal compliance. Teachers need to critically assess and discuss the value and validity of different data sources, as well as the appropriateness of established methods for data analysis.

- **Facilitating students' data literacy:** Students need skills to analyse and interpret data relevant to their learning. This includes understanding statistical graphs to understand their learning trajectory, and arguments for pursuing particular learning pathways. Students need to be aware that digital systems collect and process multiple types of their data (e.g. personal, behavioural and contextual data) to create user profiles. They should also support children to know how their data are then used, for example, to suggest learning paths or to predict their success (or failure) based on algorithms. Teachers should give students practical and experience-based advice on how to safeguard their personal data and mitigate risks related to safety and privacy in digital environments. Teachers should be able to use different activities and projects to help students learn about the ethics of data use in education, including how data systems can direct learning and impact human rights

- **Awareness of data governance architecture and legal compliance:** Teachers also need awareness around the main principles of data governance and ownership to inform and protect their learners' privacy and rights. Teachers should be able to identify both the positive and negative implications of the use of data and weigh the benefits and risks before allowing third parties to process personal data. They should know the legal and policy frameworks applicable to their school contexts and how these implicate rights to informed consent, who has access to student data, whom it is safe to share data with, how access is monitored, how long data are retained, and how data can be deleted.

- **Data-driven collaboration:** Data literacy also enables teachers to collaborate effectively with colleagues by sharing best practices, analysing data collectively, comparing and critically evaluating the credibility and reliability of data from digital environments, and collaborating on interventions to improve learning experiences and foster student achievements. Teachers should be able to present data in meaningful and accessible formats to facilitate student, parent and leadership understanding of classroom activities.

- **Environmental impact of data use:** Like school leaders, teachers should understand the environmental impact of everyday digital practices that rely on data transfer, which produces carbon emissions from devices, data centres and network infrastructures. In particular, they should understand the energy intensive processes that power digital learning environments which employ AI to operate.

Students

- **Data analysis and interpretation:**
Students need skills to analyse and interpret data relevant to their learning. This includes understanding statistical graphs to understand their learning trajectory and arguments for pursuing particular learning pathways. They need to understand how learning analytics, automated feedback and assessment, and progress monitoring may direct their learning experiences, and how their data is used in their digital learning environments and beyond.

- **Managing digital learning profiles:**
They should be aware of the benefits and dangers of integrated data systems that can track learning data over their lifetimes, understanding the opportunities this could present for recognizing competencies and learning accomplishments, as well as the repercussions it could have on their self-perception or algorithmic limitation of their future learning or employment choices. They should know the privacy policies of the learning management systems they engage with, so that they understand how their data is used to influence their learning experiences and by whom.

- **Protecting personal data:** In the digital age, students in particular need to be aware of the ethical and legal considerations surrounding the collection and sharing of their personal data as a result of their interaction with digital learning environments, including LMSs, EdTech, phone-based learning apps and participation in large-scale learning assessments. In short, anywhere where personal information is gathered and could be used and stored by a third party, students should be aware of the legal protections applicable in their contexts that safeguard their human rights. This involves an awareness of compliance procedures related to data privacy, informed consent, transparent data use and responsible cybersecurity practices in their school environments. They should understand how to use and share personally identifiable data and information while being able to protect themselves and others from the potential risks of personal information being stored by third-party users.

- **Data-driven problem solving:** As part of project-based learning, students also need data literacy skills to solve real-world problems. They should be able to collect and analyse data, draw insights, and propose solutions based on evidence. This fosters critical thinking, creativity and an understanding of the potential value of data in decision-making.

- **Environmental impact of data use:** Students,
like teachers and school leaders, should understand the environmental impact of everyday digital practices that rely on data transfer, which produces carbon emissions from devices, data centres and network infrastructures. In particular, they should understand the energy-intensive processes that power digital learning environments which employ AI.