FRENCH REPUBLIC

National Ministry of Education

Order of XX/XX/XX

defining the digital reference framework for education

NOR: XXX

The Minister for National Education,

Having regard to the Education Code, in particular Articles R421-78-3 and R421-78-4 thereof;

Having regard to the amended Order of 18 December 2017 concerning the implementation by the Ministry of National Education of a personal data processing operation known as the 'Resource Access Manager' (GAR);

Having regard to the notification to the European Commission dated XXX, pursuant to Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services;

Hereby orders:

Article 1

For the application of this Order, the following definitions shall apply:

1) 'Digital educational services': digital tools and resources made available to pupils, teachers and other members of the educational community for the purposes of teaching, learning and communication between them;

2) 'Educational digital identity': data used to identify and authenticate individuals within the information system and to authorise them to access the various digital services provided to them;

3) 'Core services': digital services made available by the State at national level to ensure the pooling of fundamental technical functions for the information system;

4) 'Digital service providing timetable functions': a digital service used to generate and manage the educational organisation framework for schools. It provides a time-and-location-based description of how lessons, optional activities and support measures are organised within the school.

5) 'Digital service supporting school life initiatives': a digital service designed to facilitate the monitoring of pupils' attendance and academic performance (including,

DRAFT

in particular, absences, marks, assessments and school reports), managed by the staff responsible for activities organised during school hours;

6) 'Digital Workplace' (ENT): an integrated suite of digital services made available, through a regional initiative, to the school's educational community, providing a unified platform to support all of the school's teaching, communication and collaboration activities;

7) 'Reference frameworks of the digital technology doctrine for education': documents setting out the rules, requirements and recommendations relating to security, interoperability and responsible digital use (eco-responsibility, digital accessibility, compliance with the legal framework on data, the protection of staff and users, and the use of artificial intelligence in educational digital services).

Article 2

Pursuant to Article R421-78-3 of the Education Code, the information systems, services and digital tools implemented in state lower and upper secondary schools in the performance of their educational duties shall comply with the reference frameworks of the digital technology doctrine for education set out in Annexes 1 to 3, in accordance with the procedures and within the timeframes specified in Annex 4.

Article 3

Pursuant to Article R421-78-4 of the Education Code, state lower and upper secondary schools shall use the following digital services, known as 'core services', in accordance with the procedures and within the timeframes set out in Annex 4:

- '**ÉduConnect':** a digital identity portal for the education sector, designed to ensure the identification and authentication of pupils and their legal guardians for access to digital services;

- '**Agents portals**': digital identity portals for the education sector – to ensure the identification and authentication of National Education staff for access to digital services;

- **'Scope'**, to facilitate the flow of educational planning data;

- '**Resource Access Manager' (GAR)**: to ensure that pupils, teachers and staff involved in the educational activity have access to digital educational resources;

- **'National Digital Audience Measurement System' (DNMA):** for measuring the audience and usage of digital services in order to collect the statistical data needed for the management of the education system.

Article 4

The provisions of this Order shall apply in the Wallis and Futuna Islands.

Article 5

This order shall be published in the Official Journal of the French Republic.

Done on

The Minister for National Education,

For the Minister and by delegation:

The Director for Digital Technology in Education,

Audran LE BARON

ANNEX 1: General Security Framework for Educational Digital Services.

ANNEX 2: Interoperability Framework for Digital Services in Education

ANNEX 3: Reference Framework for Responsible Digital Technology in Education

ANNEX 4: The conformity criteria by type of service concerned and associated application deadlines

DRAFT

ANNEX 1: General Security Framework for Educational Digital Services.

Table of contents

1. PREAMBLE 5
   1.1. Background 5
   1.2. Objectives of the document 5
   1.3. Document life cycle and governance 6
2. DIGITAL SECURITY GUIDELINES FOR EDUCATION FORMING PART OF THE TECHNICAL DOCTRINE 7
   2.1. Regarding accreditations 7
   2.2. With regard to security checks or audits in accordance with the technical reference frameworks 7
   2.3. On security clauses in contracts 8
   2.4. With regard to the management of digital security incidents 8
   2.5. In relation to an operational digital security policy 9
3. IMPLEMENTATION: RELEVANT LEGISLATION 10

DRAFT

1. Preamble

1.1. Background

This document forms part of the reference frameworks of the digital technology doctrine for education, specifically in the area of digital security. Its purpose is to provide each stakeholder involved in a project, according to their remit, with a general framework for carrying out the actions required to guarantee the security of services for Education as a whole, in coordination with the other competent authorities and in a manner consistent with the overall doctrine.

Generally speaking, every organisation – whether an institution, an operator or an IT department – and every type of application can present its own specific security challenges and, consequently, require different operational measures. Nevertheless, the digitisation of procedures, the interconnection of different information systems, the use of the same data by heterogeneous systems, and the availability of online services, combined with the sharp rise in cyber-attacks, all contribute to making digital security a global and shared challenge, which must be promoted collectively within the context of this doctrine.

1.2. Objectives of the document

The primary objective of digital security is the implementation of technical, organisational and procedural measures to ensure the protection of systems and persons. The responsibilities of the various stakeholders, who share security-related competences both legally and technically, must be exercised in accordance with the principle of subsidiarity.

Consequently, the committee structures that need to be established to ensure information-sharing represent an essential area to be developed for each scope at the outset of the system design process, enabling local teams and cross-functional teams to be connected.

From a legal and regulatory perspective, sets of rules may be common to all stakeholders (GDPR, EIDAS[1], SREN[2], specific codes, etc.) or differ in form but converge in substance. These joint efforts are aimed at achieving comprehensive security, which should be promoted by each party within their respective scope and in accordance with the relevant regulatory framework.

Thus, Act No 2013-595 of 8 July 2013 on guidelines and planning for the reform of the French education system applies across all areas and stipulates that the maintenance and IT equipment of local public educational establishments (EPLE) are the responsibility of local authorities, with the exception of digital services contracted directly by the headteacher. Consequently, local authorities are responsible for IT architecture matters

[1] https://cyber.gouv.fr/le-reglement-eidas-n9102014

[2] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049563368

DRAFT

within the scope of individual institutions, as well as for shared services and the operational aspects of the various information systems.

The areas of knowledge-sharing and exchange that enable the pooling of expertise in digital security fall into five categories:

- accreditation of information systems or applications,
- security checks or audits in accordance with technical standards,
- security clauses in contracts.
- digital security incident management,
- the common digital security operational policy.

1.3. Document life cycle and governance

The Ministry and its decentralised departments as well as local and regional authorities have been involved in the development of this general framework.

This document constitutes the third version of the General Digital Services Security Framework for Education.

An annual review, involving all relevant stakeholders, including staff and user representatives, enables an assessment of whether the document requires updating. The latter is then submitted to the Higher Council for Education (CSE) for its opinion.

DRAFT

2. Digital security guidelines for education forming part of the technical doctrine

2.1. Regarding accreditations

The Ministry is required to accredit its information systems and related digital services in accordance with a number of standards, and to provide the minimum set of requirements necessary to enable the authorities to encourage users to make use of these services, on the understanding that appropriate security measures have been assessed by the relevant committees.

This is reiterated in several regulatory documents (RGS, PSSIE, interministerial or ministerial instructions). The competent authorities responsible for information system security and the accreditation authorities required to carry out these projects are appointed by regulation.

The accreditation files address GDPR compliance, both in terms of register entries and potential data protection impact assessments. More generally, all stakeholders involved in the construction and operation of digital services are bound by the GDPR.

It should be noted that compliance with the GDPR also entails – by virtue of the principles of data minimisation that it emphasises – the conditions for reducing the environmental footprint. It seems appropriate to link the two concepts in the work so as to take into account jointly the requirements of the two areas.

NO 1	Rule The competent authorities responsible for information system security shall implement accreditation procedures for the digital services under their remit and are inviting the relevant security departments of partner authorities to share information regarding the certification committees.

2.2. With regard to security checks or audits in accordance with the technical reference frameworks

With regard to monitoring compliance with the security standards published by ANSSI or the CNIL, technical audits should be drawn up jointly by the relevant stakeholders, in particular the technical departments of local authorities and those of the academic region, with a view to convening an accreditation committee in which each party is represented. These regular audits are included in the files of the accreditation committees and also provide an opportunity to work together to improve the security of the information systems that support the provision of digital services for education.

DRAFT

No 2	Rule Technical audits of digital services for education are designed and carried out jointly by academic technical teams, partner teams and third-party stakeholders involved in the provision of these services. These teams may jointly commission external audits on a contracted basis where necessary. A framework document setting out the minimum control and audit requirements, applicable to all entities operating information systems that provide digital services for education, will be drawn up by a working group comprising various stakeholders in the sector.

2.3. On security clauses in contracts

When digital services for education are developed through services procured via public contracts, regulatory requirements relating to the security of information systems must be taken into account from the very outset of the drafting of the tender specifications, so that the contract can be carried out in such a way as to enable the teams responsible for implementation to commission the appropriate services. It is therefore essential to share information in advance regarding the security provisions of information systems when drafting tender specifications, to ensure that the contract proceeds smoothly thereafter.

In particular, these joint efforts help to harmonise best practices in information system security—as laid down by law or regulation—that apply across the various areas of activity of digital service providers in the education sector.

No 3	Rule Security clauses in contracts are drawn up jointly by the technical teams working on the development of digital services for education, to ensure that all existing services are operated securely.

2.4. With regard to the management of digital security incidents

The handling of major incidents is a joint process between the academic ISSRs, which are responsible for reporting digital security incidents to the Ministry’s Information Systems Security Operational Centre (Cossim), and the ISSRs of local and regional authorities.

Every head teacher, even without being an AQSSI, acts as the point of contact for digital security for the decentralised departments of the national education system, and in particular for the alert chain within the scope for which they are a user or for which they are responsible, especially in the event of a digital security incident that significantly affects the activities of their institution.

To this end, each academy maintains a directory of points of contact in EPLEs.

The academic RSSI informs and engages the Cossim so that the information is handled within the broader context of incidents affecting the Ministry, in liaison with the Ministry's decision-making authorities, and with ANSSI and law enforcement where necessary.

DRAFT

It is essential that the Ministry’s decision-makers are fully aware of any security incidents occurring across all digital services for education as soon as they arise, so that they can manage their impact, disseminate information on new threats to all IT stakeholders, whether they operate within the scope of digital resources for education or in related areas, including local authority teams for their own purposes.

It is essential to work together in dealing with and managing incidents, as a swift response to new attack scenarios is key to limiting the impact of such attacks and even to thwarting them entirely through prevention or by raising awareness amongst all stakeholders.

No 4	Rule Security incidents must be reported through the appropriate alert channels in accordance with the incident reporting procedures distributed to all stakeholders in digital services for education.

2.5. In relation to an operational digital security policy

The definition of operational policies has been the subject of extensive sector-specific work (across industrial sectors, administrative areas, business lines and specialisms) and has helped to clarify for all stakeholders what is expected and what constitutes best practice, whether in the design of architectures, the operation of information systems or the development of applications.

In the shared management of data processing within digital services for education, the interconnection of information systems through the integration of different domains means that changes are addressed jointly in line with requirements and specifications, as well as through remedial actions following incidents and alerts. It is therefore appropriate to define a framework that can guide all stakeholders in developing future digital services and managing existing ones.

Such a general framework will be reviewed regularly through a comitology process comprising stakeholders in the digital education sector and those involved in information systems security, and submitted for validation to the partners' committee.

No 5	Rule Technical teams working in the field of digital technology for education shall work together with the digital security teams at the Ministry and local authorities to draw up an Operational Digital Security Policy (POSN), which sets out a body of technical rules to be followed in the secure development, operation and organisation of digital services for education.

DRAFT

3. Implementation: relevant legislation

The process of securing information systems, like all digital security procedures, is underpinned by the relevant legislation and regulations.

As a reminder, the legislation relating to the various areas is listed below; it should be noted that these bodies of legislation are consistent with the requirements of the doctrine set out above.

General regulatory framework applicable to digital services and infrastructure operated by the Ministry, its decentralised departments and public bodies under the Ministry's supervision, as well as the service providers involved

The legislation relating to digital technology, digital security, and information and communication systems applicable to ministries, decentralised departments and public bodies under the Ministry's supervision is as follows:

- Decree No 2022-513 of 8 April 2022 on the digital security of the information and communication system of the State and its public institutions (NOR: PRMD2135717D).
- Order of 26 October 2022 approving Joint Ministerial General Instruction No 1337/SGDSN/ANSSI on the organisation of the digital security of the information and communication system of the State and its public establishments (NOR: PRMD2221955A).
- Decree No 2019-1088 of 25 October 2019 on the State Information and Communication System and the Interministerial Directorate for Digital Technology (NOR: PRMG1929496D).
- The General Security Framework adopted pursuant to Decree No 2010-112 of 2 February 2010, implementing Articles 9, 10 and 12 of Ordinance No 2005-1516 of 8 December 2005 on electronic interactions between users and administrative authorities and between administrative authorities (NOR: PRMX0909445D).
- Order of 13 June 2014 approving the General Security Framework and specifying the procedures for implementing the electronic certificate validation procedure (NOR: PRMD1413745A).
- Prime Minister's Circular No 5725/SG of 17 July 2014 introducing the State Information Systems Security Policy (PSSIE) (NOR: PRMX1420095C).
- Joint Ministerial Instruction No 901/SGDSN/ANSSI on the protection of sensitive information systems (NOR: PRMD1503279J). Ordinance No 2005-1516 of 8 December 2005 on electronic interactions between users and administrative authorities and between administrative authorities (NOR: ECOX0500286R).
- Ordinance No 2017-1426 on electronic identification and trust services for electronic transactions (NOR: PRMD1724021R).

Legislation relating to personal data protection

DRAFT

- Law No 2018-493 of 20 June 2018 on personal data protection (NOR: JUSC1732261L).
- Decree No 2019-536 of 29 May 2019 implementing Law No 78-17 of 6 January 1978 on information technology, files and freedoms, in particular Article 85 and Articles 140 et seq. (NOR: JUSC1911425D).

Legislation concerning specific areas

- Order of 13 July 2020 laying down the safety rules and procedures for reporting information systems of vital importance and security incidents relating to the 'Public research' subsector of activities of vital importance (NOR: (PRMD2018060A) and its annexes.
- Decree No 2018-384 of 23 May 2018 on the security of information networks and systems for essential services (NOR: PRMD1809740D).
- Order of 14 September 2018 laying down the security rules and time limits referred to in Article 10 of Decree No 2018-384 of 23 May 2018 on the security of information networks and systems of operators of essential services and digital service providers (NOR: PRMD1824939A).
- Decree No 2011-1425 of 2 November 2011 implementing Article 413-7 of the Criminal Code and relating to the protection of the scientific and technical potential of the nation (NOR: PRMX1118649D).
- Order of 3 July 2012 on the protection of the nation's scientific and technical potential (NOR: PRMX1227979A).
- Inter-ministerial Circular No 3415/SGDSN/AIST/PST of 7 November 2012 on the implementation of the mechanism for the protection of the nation's scientific and technical potential (NOR: PR1vID1238889C).

Legislation on the protection of national defence secrets

- Order of 9 August 2021 approving Interministerial General Instruction No 1300 on the protection of national defence secrets (NOR: PRMD2123775A).

Legislation on the government's organisational structure for the management of major crises

- Circular No 6095/SG of 1 July 2019 regarding the government's organisational structure for the management of major crises.

General regulatory framework for digital services and infrastructures operated by local and regional authorities and their providers

In the document 'Sécurité numérique des collectivités territoriales[3]', ANSSI reiterated the need to maintain accreditations and comply with the GDPR.

[3] https://cyber.gouv.fr/sites/default/files/2020/01/anssi-guide-securite_numerique_collectivites_territoriales-reglementation1.pdf

DRAFT

Thus, the legislation relating to digital technology, digital security, and information and communication systems applicable to digital services and infrastructure operated by local authorities and service providers includes, in particular, the following laws and regulations:

Legislation relating to digital technology, digital security, and information and communication systems

- The General Security Framework adopted pursuant to Decree No 2010-112 of 2 February 2010, implementing Articles 9, 10 and 12 of Ordinance No 2005-1516 of 8 December 2005 on electronic interactions between users and administrative authorities and between administrative authorities (NOR: PRMX0909445D).
- Order of 13 June 2014 approving the General Security Framework and specifying the procedures for implementing the electronic certificate validation procedure (NOR: PRMD1413745A).
- Ordinance No 2005-1516 of 8 December 2005 on electronic interactions between users and administrative authorities and between administrative authorities (NOR: ECOX0500286R).
- Ordinance No 2017-1426 on electronic identification and trust services for electronic transactions (NOR: PRMD1724021R).

DRAFT

ANNEX 2: Interoperability Framework for Digital Services in Education

Table of contents

1. Preamble 17
   1.1 Background 17
   1.2 Objectives of the document 17
   1.3 Document life cycle and governance 18
2. Interoperability principles 19
   2.1. Definition 19
   2.2. Interoperability levels 20
   2.3. Nomenclatures and vocabularies 22
   2.4. Principles and tools for data exchange 22
3. Scope and principles of the interoperability framework for digital services in education 27
   3.1. Interoperability scope 27
   3.2. Typology of education data 27
   3.3. Benefits of interoperability for users 28
   3.4. Standard selection criteria 30
4. Data mapping and standardisation needs 31
5. Common information architecture principles 33
   5.1. Education object nomenclatures 33
   5.2. Data exchange via API 34
   5.3. File exchanges for storage systems 34
   5.4. Standards 35
6. Presentation of selected requirements and standards by functional area 37
   6.1. User identification and authentication in an interoperable environment 37
   6.2. Educational organisation for school life 40
   6.3. Digital service portals and digital resources and services for teaching and educational practices 43
   6.4. Exams, certifications and competitions 46
   6.5 Management of educational missions 47
7. Summary of the selected standards 49
8. Use case 55
   8.1. Access an educational resource 55
   8.2. Facilitate the integration of resources into an LMS for seamless use in an education path 56
   8.3 Ensure portability of the content of an education path when changing LMS 57

DRAFT

DRAFT

List of figures

Figure 1: Definitions and interoperability levels.....21

Figure 2: Data organisation design.....24

Figure 3: Standard data description grid.....27

Figure 4: Four areas for improvement.....28

Figure 5: Data standardisation needs assessment grid.....31

Figure 6: Positioning of nomenclatures.....33

Figure 7: Summary of the selected standards.....50

DRAFT

1. Preamble

1.1 Background

This document constitutes the Interoperability Framework for Digital Services in education. It forms part of the body of the reference frameworks of the digital technology doctrine for education

It sets out the rules, requirements and recommendations for interoperability for all stakeholders involved in the provision of digital services for education.

This document is based on French and European reference documents: the[4] general interoperability framework and [5]the European Interoperability Framework (EIF). It is inspired by best practices in standardisation, technical architecture and Information systems architecture planning. It does not subscribe to any proprietary methods or tools.

This document is specifically intended for those who develop, operate and integrate digital services for education on behalf of project sponsors and data controllers (local authorities, regional education authorities, the Department for Education, and local education authorities). Its aim is to ensure that every stakeholder can provide value-added services under the same rules, and that every user can benefit from these services within the framework of trust established by the Ministry in its reference frameworks of the digital technology doctrine for education.

1.2 Objectives of the document

The purpose of the document is to define interoperability **requirements** for digital services for education.

It must thus facilitate **the choices for designers and buyers** of digital services for education, and **enhance the coherence of the digital ecosystem for education at national and European level.**

The document therefore defines the **standards and protocols** of the scope defined in the technical doctrine. Future versions of the document may also set out trajectories and targets to be achieved within a specified timeframe.

DRAFT

[4] General Interoperability Framework Version 2.0 – December 2015:
https://www.numerique.gouv.fr/uploads/Referentiel_General_Interoperabilite_V2.pdf

[5] https://joinup.ec.europa.eu/collection/interoperable-europe/interoperable-europe

1.3 Document life cycle and governance

The Ministry, its decentralised services and operators, local and regional authorities and digital education service providers participated in the development of this reference framework. Teachers and school management staff were also involved in the work to identify users' needs regarding improvements to their user experience within the ecosystem of digital services and resources for education available to them.

This document constitutes the third version of the Interoperability Framework for Digital Services in Education

This document is intended to be updated regularly to keep pace with future technological and legal developments. An annual review, involving all relevant stakeholders, including staff and user representatives, enables an assessment of whether the document requires updating. The latter is then submitted to the Higher Council for Education (CSE) for its opinion.

DRAFT

2. Interoperability principles

Interoperability, which extends beyond purely technical considerations, affects IT systems, processes, procedures and organisations throughout their entire lifecycle. Interoperability is ensured through standards and formats that must be adhered to by any component or system wishing to be part of an interoperable environment. While interoperability in the fields of IT and telecommunications can also serve as a tool for competitive positioning, enabling consortia to collaborate in order to offer more comprehensive services that complement one another, it is also a tool designed to benefit people by providing them with smoother user experiences that are better tailored to their needs.

2.1. Definition

Interoperability refers to the ability of two or more systems to exchange data and utilise each other’s information without requiring significant effort on the part of users or developers to integrate and make use of them.

To do this, these systems must first agree on how they will communicate and use the data and information that can be exchanged. This involves agreeing on the exchange protocols to be used, as well as the format, meaning, relevance and added value of the data exchanged.

Identity and access management based on shared rules enables the provision of user journeys that do not require re-authentication and respect personal data, thereby addressing an initial need for interoperability between systems. Shared business concepts and processes, meanwhile, lay the foundations for interoperability requirements for stakeholders operating within the same business domain. The adoption of identical standards within an ecosystem promotes technological autonomy among its various systems. By complying with a standardised interface, one system can be replaced by another almost seamlessly.

The interoperability approach between systems:

- enables simplified and streamlined communication and collaboration between different applications, platforms or information systems,
- encourages innovation and creativity in developing new features for users, whilst facilitating the scalability of systems that comply with the relevant interfaces,
- promotes complementarity and fair competition between systems within the ecosystem,
- prevents the proliferation of specific connectors and helps to keep costs under control for all stakeholders.

DRAFT

Interoperability is therefore crucial in order to harness the benefits offered by various technologies to create more flexible, fluid and efficient IT environments for the end-user.

2.2. Interoperability levels

As identified by the EIF (European Interoperability Framework)[6] and reiterated in the RGI (General Interoperability Framework), several levels of interoperability must be taken into account whenever two systems are to communicate with one another.

DRAFT

[6] https://joinup.ec.europa.eu/collection/interoperable-europe/interoperable-europe

Niveau politique : Des VISIONS PARTAGEES ET DES STRATEGIES CONVERGENTES favorisent les échanges entre parties prenantes

Niveau juridique : Alignement juridique garantissant que les données échangées sont en accord avec le CADRE LEGAL ET LES ACCORDS CONTRACTUELS établis entre les parties

Niveau organisationnel : Définit les MOYENS mis en œuvre et l'ORGANISATION nécessaire pour favoriser les échanges

Niveau sémantique (savoir se faire comprendre) : Définit la SIGNIFICATION DES DONNEES échangées dans un souci de préservation de leur signification et d'une compréhension partagée

Niveau syntaxique (savoir communiquer) : Définit la SYNTAXE DES ECHANGES. La syntaxe traduit le sens en symboles.

Niveau technique (Pouvoir communiquer) : Précises les CARACTERISTIQUES de la communication

Policy level: SHARED VISIONS AND CONVERGENT STRATEGIES foster dialogue among stakeholders

Legal level: Legal alignment ensuring that the data exchanged is in agreement with the LEGAL FRAMEWORK AND CONTRACTUAL AGREEMENTS established between the Parties

Organisational level: Sets out the RESOURCES deployed and the ORGANISATION required to facilitate exchanges

Semantic level (ability to make oneself understood): Defines the MEANING OF THE DATA exchanged in order to preserve its meaning and ensure a shared understanding

Syntactic level (ability to communicate): Defines the EXCHANGE SYNTAX. Syntax translates the meaning into symbols.

Technical level (Ability to communicate): Specifies the CHARACTERISTICS of the communication

Figure 1: Definitions and interoperability levels

1. The political level provides a convergent strategy and shared visions among stakeholders, thus promoting the implementation of exchange solutions.

DRAFT

2. The legal level ensures that the information exchanged will be in accordance with the legal and regulatory framework and contractual agreements established. In particular, it must take into account the recommendations of the CNIL and ANSSI.
3. The organisational level defines the resources and procedures put in place to enable data exchange and interoperability between systems.
4. The semantic level allows for a shared understanding of the different elements of the exchange between the relevant parties. This will allow it to be based on a set of nomenclatures shared between the stakeholders.
5. The syntactic level specifies the format of the exchanged data.
6. Finally, the technical level defines the technical characteristics of the exchange, such as the protocols and means of transport.

2.3. Nomenclatures and vocabularies

Interoperability between heterogeneous services or information systems and in exchange systems requires the creation and maintenance of information that is intellgible to all parties.

Semantic interoperability specifications require the definition of a common language that enables applications within participating information systems to interpret the nature and values of the transmitted data in a consistent manner and to reuse it without error or loss of information.

Within the field of education, different nomenclatures enable this need to be met.

The nomenclatures of the BCN (Central Nomenclature Database) form the common language of the information system used by the Ministry of Education. They are updated regularly and tracked historically by means of opening and closing dates. They are available for consultation on the website of the Central Nomenclature Database:[7].

In addition to its application profile, ScoLOMFR[8] provides stakeholders with shared vocabularies covering the key aspects of school activities and teaching. It is available to the entire school community.

2.4. Principles and tools for data exchange

To ensure that data is exchanged between stakeholders under the right conditions, thereby guaranteeing effective interoperability, certain principles must be agreed upon and adhered to.

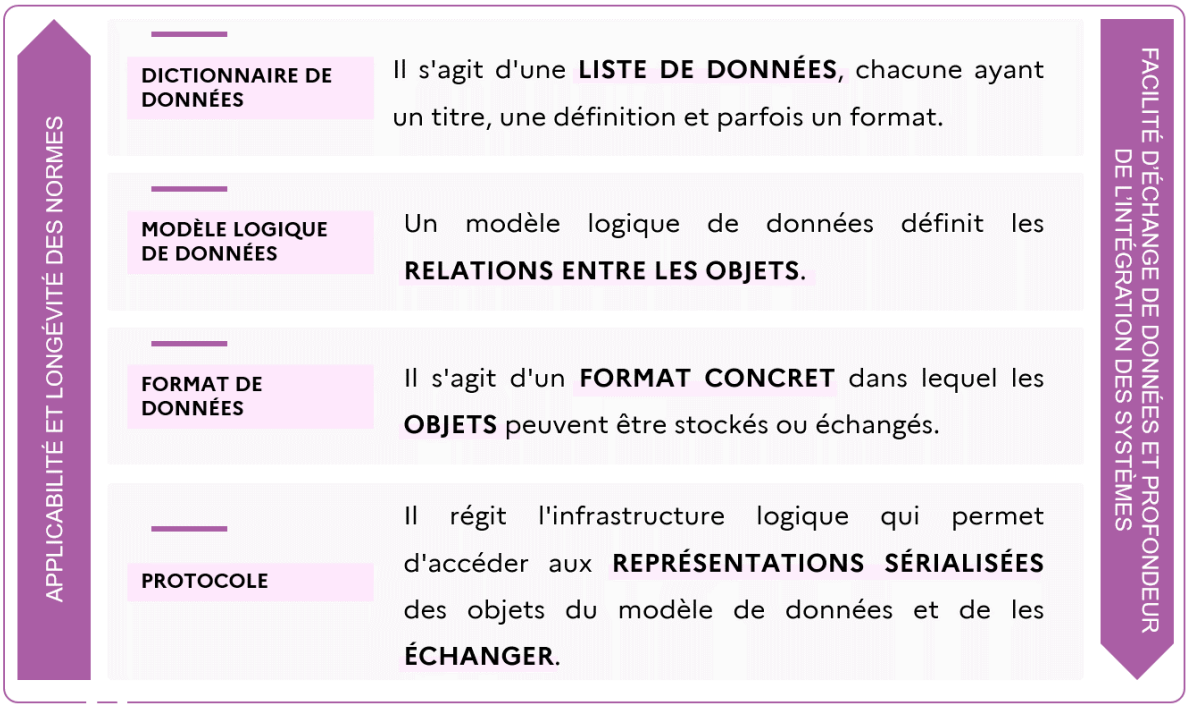
It is therefore possible to develop tools to implement these principles, based on APIs, the large-scale management of which for service integration can be facilitated through the use of an API management platform.

[7] http://infocentre.pleiade.education.fr/bcn/

[8] https://eduscol.education.fr/1086/le-referentiel-scolomfr

2.4.1. A coherent set, from data dictionary to recommended protocols

The proposal shown below is inspired by the work of Brandt Redd[9], which is published on EdMatrix[10] under a Creative Commons 4.0 licence. The design of the data requires a four-layer organisation. They are not necessarily included in all standards, but each one must be taken into account in order to form part of a functional system.



Applicabilité et longévité des normes
Dictionnaire de données : Il s'agit d'une LISTE DE DONNES, chacune ayant un titre, une définition t parfois un format.
Modèle logique de données : Un modèle logique de données définit les RELATIONS ENTRE LES OBJETS.
Format de données : Il s'agit d'un FORMAT CONCRET dans lequel les OBJETS peuvent être stockés ou échangés.
Protocole : Il régit l'infrastructure logique qui permet d'accéder aux REPRESENTATIONS SERIALISEES des objets du modèle de données et de les ECHANGER
Facilité d'échange de données et profondeur de l'intégration des systèmes

Applicability and longevity of standards
Data dictionary: This is a LIST OF DATA ITEMS, each item having a title, a definition and, in some cases, a format.
Logical data model: A logical data model defines the RELATIONSHIPS BETWEEN OBJECTS.
Data format: This is a CONCRETE FORMAT in which OBJECTS can be stored or exchanged.

Protocol: It governs the logical infrastructure that enables access to and exchange of the SERIALISED REPRESENTATIONS of the data model objects
Ease of data exchange and depth of systems integration

Figure 2: Data organisation design

[9] https://brandtredd.org/

[10] https://www.edmatrix.org/

Data dictionary: This is a list of data items, each with a title, a definition and, in some cases, a format. For example, Title: ‘Date de naissance’; Definition: ‘Day of birth of an individual’; Format: ‘year-month-day’.

Logical data model: A logical data model defines the structure of the data by describing the relationships between data items, which are grouped into coherent sets (objects or entities). For example, a ‘Student’ entity may include properties such as ‘Name’, ‘Date of birth’, ‘Sex’, ‘Address’ etc. The ‘Student’ entity type would have a **many-to-many** relationship with the ‘Class’ entity.

Data format: This involves encoding information that represents an object in the form of a sequence of smaller (‘atomic’) units of information, in order to enable the transmission or storage of structured data. XML and JSON, for example, are competing formats for text-based encoding, but custom formats may also exist and be applied to the same data model.

Protocol: It dictates the rules of communication between two systems to ensure that the exchanged data is sent and received without loss of bytes, without error, without duplication and in the order in which it was sent.

2.4.2. Implementing API-based exchanges

While a protocol is a set of rules that govern how data is transmitted over a network, an API is an interface that allows two different applications to communicate with each other. Implementing data exchange via APIs ensures seamless interaction between applications, services and resources, and enables the effective integration of digital services from one or more platforms into a navigation experience optimised for pupils, teachers or any other member of the educational community. This facilitates collaboration and resource sharing.

APIs must be accompanied by comprehensive and clear documentation from the provider, as well as effective technical support, in order for developers to easily integrate and use them.

They are designed to be flexible and scalable so that they can meet current needs and adapt to future requirements.

DRAFT

3. Scope and principles of the interoperability framework for digital services in education

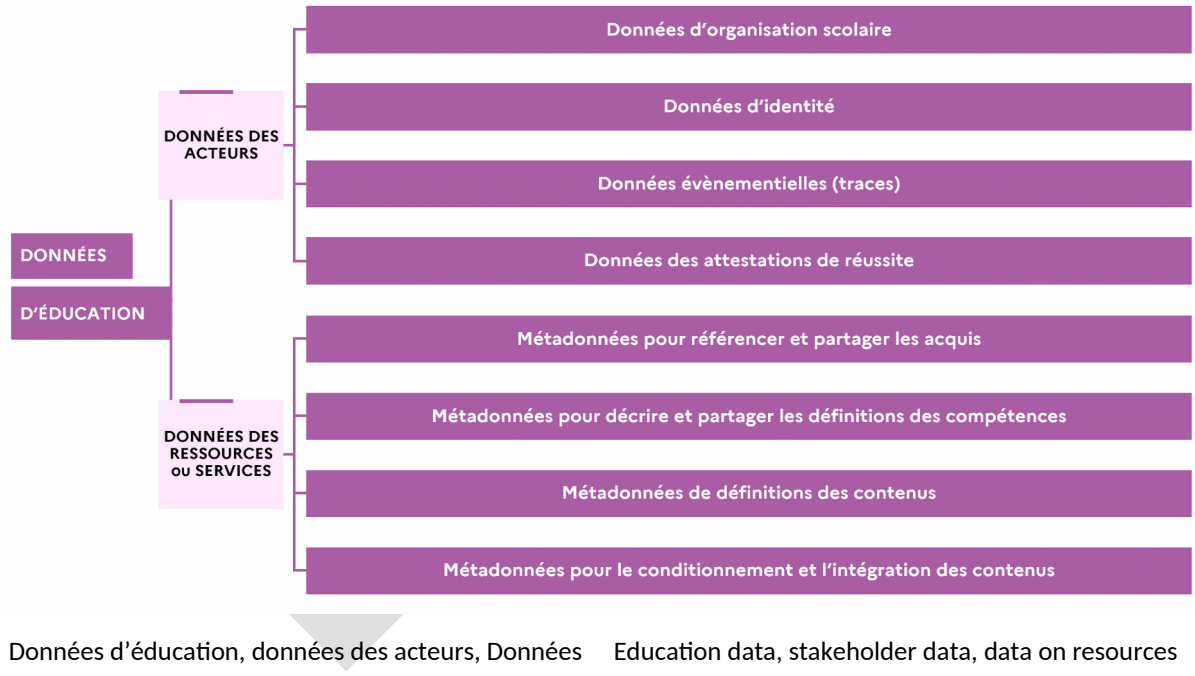
3.1. Interoperability scope

The Interoperability Framework for Digital Education Services addresses interoperability issues across all digital education services provided by public or private sector organisations.

3.2. Typology of education data

In order to establish common rules for the interoperability of digital services, the diagram below sets out a standard data description framework, based on the classification of education data presented in Chapter 5 of the technical guidelines.

These proposals and illustrations are inspired by the work of Brandt Redd, which is published on EdMatrix under a Creative Commons 4.0 licence.



Données d'éducation, données des acteurs, Données des ressources ou services	Education data, stakeholder data, data on resources or services
Données d'organisation scolaire	Data on school organisation
Données d'identité	Identity data
Données événementielles (Traces)	Event data (logs)
Données des attestations de réussite	Data on attestations of achievement
Métadonnées pour référencer et partager les acquis	Metadata for cataloguing and sharing knowledge
Métadonnées pour décrire et partager les définitions des compétences	Metadata to describe and share competency definitions
Métadonnées de définitions des contenus	Content definition metadata
Métadonnées pour le conditionnement et l'intégration des contenus	Metadata for conditioning and content integration

Figure 3: Standard data description grid

DRAFT

Standard education data can be divided into two main categories and eight types:

- Stakeholder data
  - Data describing the school organisation
  - Identity-related data
  - Data describing interactions between participants (event data), including ‘learning traces’
  - Descriptive data on certificates of achievement
- Data relating to content (‘resource or service data’)
  - Metadata for the certified referencing and sharing of individuals’ learning outcomes
  - Metadata to describe, reference and share competency definitions
  - Content definition metadata
  - Metadata for conditioning and integration of content.

3.3. Benefits of interoperability for users

The framework aims to contribute to the development of a **coherent overall service offering, focused on users' needs**.

Work carried out with users of digital education services[11] as part of the 2023–2024 work programme for the Digital Technical Doctrine has identified four areas for improvement relating to interoperability between services.

Authentification unique des utilisateurs	Single sign-on for users
Portabilité des données spatio-temporelle	Time-and-location-based data portability
Circulation des données entre SNE	Data circulation between SNEs
Intégration de contenus entre SNE	Integration of content between SNEs

Figure 4: Four areas for improvement

3.3.1. Single authentication

Single user authentication is required for:

- ensuring easy access to digital services and facilitating seamless user journeys between services (‘tell us once’ principle)

[11] SNE: digital services for education

- contribute to the security of the service and the user journey
- contribute to the defendability of the service

The solutions (standards and core services of the scope of education described in Chapter 4 of the technical doctrine) used for authentication and the propagation of identity data have an impact on the other strands.

3.3.2. Data portability for stakeholders

Data portability must be defined at the outset of the contract; it is necessary to:

- ensure continuity in the user journey across school years and cycles;
- ensure continuity of the user journey between institutions or school authorities;
- ensure the continuity of the user journey when changing service providers;
- guarantee the authenticity, integrity and availability of data, and to ensure non-repudiation;
- ensure that the data is exported in a legible format.

3.3.3. Data flows between digital services

The controlled flow of data between digital services for education is necessary to:

- provide the public educational digital service for educational activities and missions and administrative procedures (‘tell us once’ principle);
- create new features that benefit users and the ecosystem;
- build on the opportunities offered by digital technology for personalising learning pathways, monitoring learning progress and providing remedial support by enhancing the tools available;
- monitor the pupil’s progress, regardless of the activity they have completed and regardless of which provider offers the relevant digital service;
- ensure the preservation, maintenance of the integrity, authenticity and non-repudiation of the data produced by the user for their own use.

3.3.4. Integration of editorial content

The integration of editorial content across digital services and resources is necessary in order to:

- create seamless user journeys;
- promote synergy between services.

DRAFT

3.4. Standard selection criteria

In line with the adoption criteria for the RGI[12], the standards selected in this document meet the following criteria:

- open,
- relevant,
- mature,
- independent,
- easy to deploy,
- supported by the industry.

In addition, each standard is associated with a status to help service providers take it into account, allow for a transition period and achieve progressive compliance. The 'emerging' status also allows technological innovations to be taken into account.

Status	Status explanation
Target	This is a standard that must be observed and applied by everyone.
In use	This is a standard currently in use within education information systems.
Emerging	This is an emerging standard, or one whose maturity, implementation and support from the research community and/or industry are not yet fully established.
End of life	This is an end-of-life standard, whose support ends because other replacement standards are emerging. Its application must be taken with caution and is therefore considered to be 'on hold'. If its removal has not yet been requested in all existing systems, it must not, however, be used for new projects.

DRAFT

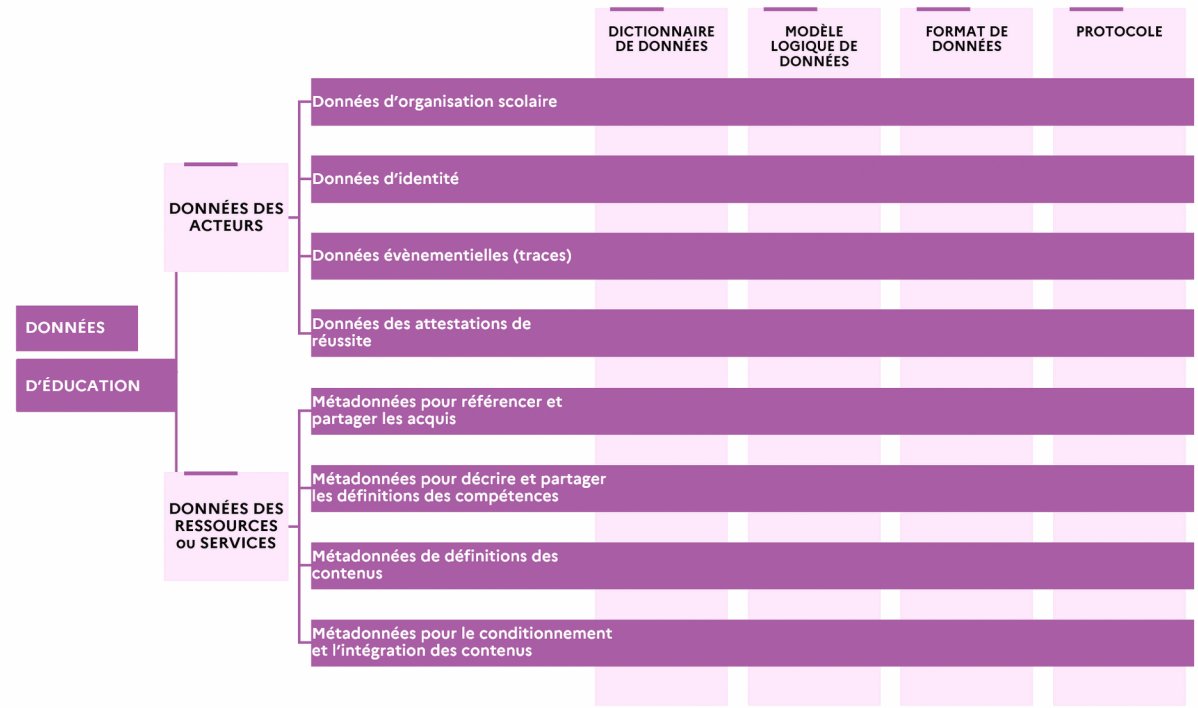
[12] General Interoperability Framework Version 2.0 – December 2015: https://www.numerique.gouv.fr/uploads/Referentiel_General_Interoperabilite_V2.pdf

4. Data mapping and standardisation needs

To ensure that data exchanges between stakeholders enable effective interoperability, certain principles must be agreed upon and adhered to. Based on the data typology presented in Chapter 2 of this document, the matrix below provides a framework for identifying data standardisation requirements.

It highlights the need for shared data dictionaries, rules for structuring data, and for exchanging data in accordance with common principles, so that data can be exchanged in the most efficient way possible and in the user's best interests.

Chapter 6 describes the standards adopted in the reference frameworks of the digital technology doctrine for education, and then summarises them using the same matrix.



Données d'éducation, données des acteurs, Données des ressources ou services	Education data, stakeholder data, data on resources or services
Données d'organisation scolaire	Data on school organisation
Données d'identité	Identity data
Données événementielles (Traces)	Event data (logs)
Données des attestations de réussite	Data on attestations of achievement
Métadonnées pour référencer et partager les acquis	Metadata for cataloguing and sharing knowledge
Métadonnées pour décrire et partager les définitions des compétences	Metadata to describe and share competency definitions
Métadonnées de définitions des contenus	Content definition metadata
Métadonnées pour le conditionnement et l'intégration des contenus	Metadata for conditioning and content integration
Dictionnaire de données, Modèle logistique de données, Format de données, Protocole	Data dictionary, Logical Data Model, Data Format, Protocol

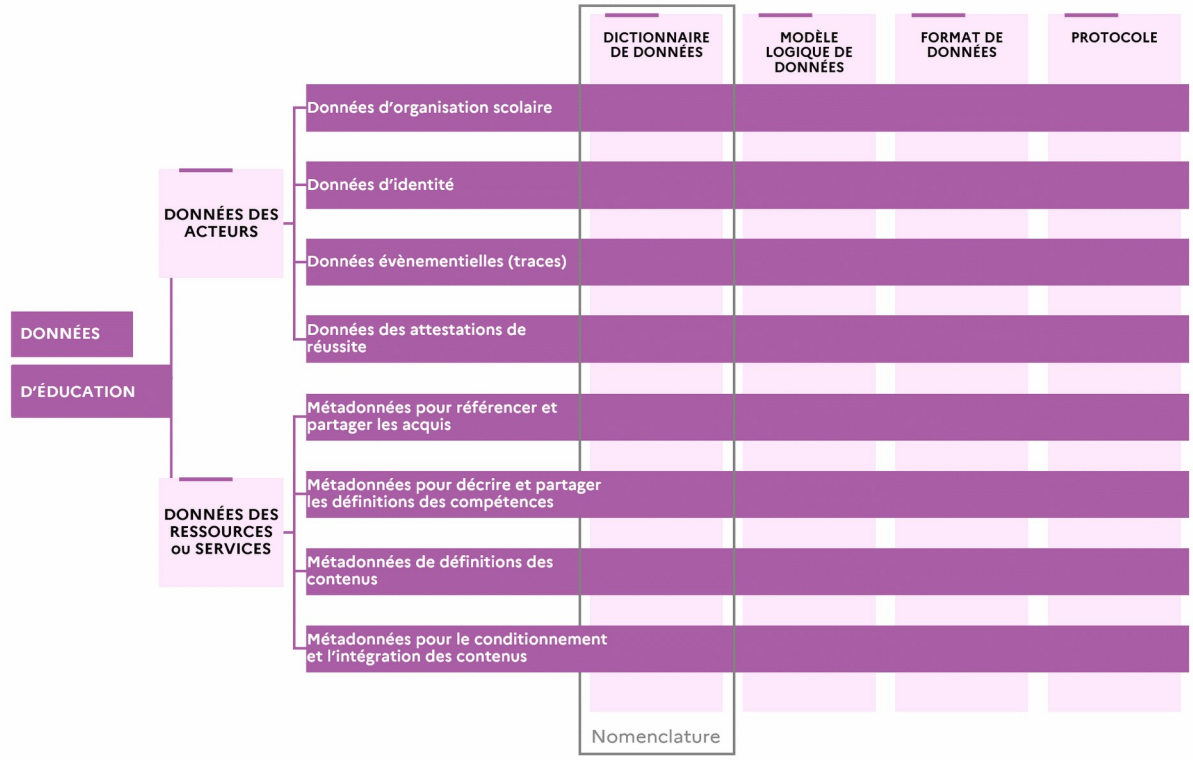
Figure 5: Data standardisation needs assessment grid.

5. Common information architecture principles

For an information architecture-based approach to data exchanges, necessary to break down silos in the digital services sector for education, common vocabularies are needed and interactions via APIs will ensure the fluidity of data exchanges and integration between services.

5.1. Education object nomenclatures.

National nomenclatures provide a basic vocabulary in French, enabling stakeholders to share a common understanding of the concept in question, regardless of the system from which it originates. These shared vocabularies are essential for improving the semantic interoperability of interconnected services.



Données d'éducation, données des acteurs, Données des ressources ou services	Education data, stakeholder data, data on resources or services
Données d'organisation scolaire	Data on school organisation
Données d'identité	Identity data
Données événementielles (Traces)	Event data (logs)
Données des attestations de réussite	Data on attestations of achievement
Métadonnées pour référencer et partager les acquis	Metadata for cataloguing and sharing knowledge
Métadonnées pour décrire et partager les définitions des compétences	Metadata to describe and share competency definitions
Métadonnées de définitions des contenus	Content definition metadata
Métadonnées pour le conditionnement et l'intégration des contenus	Metadata for conditioning and content integration
Dictionnaire de données, Nomenclature, Modèle logistique de données, Format de données,	Data dictionary, Nomenclature, Logical data model, Data format, Protocol

Figure 6: Positioning of nomenclatures

DRAFT

NO 1	Requirement The digital services for education at primary and secondary levels describe individuals and educational institutions in the same way, based on the classifications in the BCN (Central Classification Database).

5.2. Data exchange via API

No 2	Requirements Digital services for education are API-enabled by exposing secure APIs for use by other services or client applications. They also enable the use of APIs provided by third-party services or applications. The services also provide access to other services via APIs.
No 3	OMOGEN is the single entry and exit point for public data exchanges via APIs with academic information systems, with external partners and at national level.

5.3. File exchanges for storage systems

No 4	Requirement File storage systems allow the sharing and exchange of files in Object format using the REST or S3 protocol

DRAFT

5.4. Standards

The table below sets out the applicable standards and their status regarding data exchange and circulation.

Fields	Body	Standards	Comment	Status
Protocol	IETF	HTTPS	HyperText Transfer Protocol Secure: a combination of HTTP and a TLS encryption layer.	Target
Protocol		REST	Representational state transfer. Software architecture style defining a set of constraints to be used to create web services	Target
Format	IETF	JSON	JavaScript Object Notation. A text-based data format derived from the notation used for JavaScript objects.	Target
Format	W3C	XML	Extensible Markup Language. The initial objective of XML is to facilitate the automated exchange of complex content between heterogeneous information systems.	In use

DRAFT

6. Presentation of selected requirements and standards by functional area

This chapter sets out all the requirements for digital services for education, organised by functional area and data type.

6.1. User identification and authentication in an interoperable environment

User authentication is carried out by a digital ‘identification/authentication’ service that operates by receiving and verifying a ‘Identifier/authenticator’ combination. It also enables the life cycle management of identities and authenticators.

Identification is used to determine a user’s identity, whereas authentication is used to verify that identity.

There are several types of authentication: using information that only the user knows (password), possesses (smart card), is (biometric data), or can perform (a gesture).

Authentication protocols describe the interactions between a prover and a verifier, as well as the messages used to prove a user’s identity. There are two main types of authentication protocols: simple authentication (involving a single authentication factor) and strong authentication (involving two or more factors). Furthermore, the term ‘single sign-on’ refers to a situation where a user only needs to log in once to access multiple computer applications.

No 5	Requirement Digital services for education implement single sign-on (SSO) identity propagation functions. The system allows users to access an external service and then return to the original service by exchanging identity data.

DRAFT

6.1.1. Identity providers within the scope of digital services for education (core services)

Chapter 4 of the the digital technology doctrine for education describes the ÉduConnect identification and authentication services for pupils and their legal guardians, and the Agents portal for National Education staff.

They enable these users to use a single set of credentials across the various connected service portals.

6.1.2. Interface with identity provider platform services

No 6	Requirement Digital services for education use the core services for the authentication and identification of users within the education sector.

6.1.2.1. ÉduConnect Interface Contracts

ÉduConnect interface contracts are available on request during the installation work.

The interconnection of digital education services with the ÉduConnect portal, provided that they fall under the data controller responsibility of the Ministry of National Education (the Ministry, regional education authorities, school heads, and IA-DASEN) and are recorded in the data processing registers of the relevant entities, is achieved through the implementation of an identity federation.

6.1.2.2. Agents Portal Interface Contracts

Coming soon

6.1.3. Standards

No 7	Requirement For the federation of identities enabling SSO authentication, digital services for education rely on standard and proven protocols as described in the table below. API calls use authentication based on authorisation and authentication protocols such as OAuth2 or OIDC.

DRAFT

The table below shows applicable standards and their status for user identification and authentication.

Fields	Body	Standard	Comment	Status
Protocol	OIDF	Open ID Connect (OIDC)	Identification layer based on OAuth 2.0, authorisation device.	Target
Protocol	Internet engineering task force (IETF)	OAuth2	Authorisation protocol. Included in OIDC	Target
Protocol	Organization for the Advancement of Structured Information Standards (OASIS)	SAML 2.0	Used by the GAR. Enables the exchange of authentication and identification data between security domains.	In use
Protocol	APEREO	CAS	Central Authentication Service (single sign-on system) Support for OIDC, OAuth2 and SAML	End of life

DRAFT

6.2. Educational organisation for school life

The functions relating to the business processes and activities underpinned by the educational organisation are designed to define and update the school's optimised timetable, covering both spatial and temporal organisation, in order to ensure the delivery of educational services. School organisational data is required for functions relating to the monitoring of pupil attendance (absences, assessments, etc.), as defined in the Education Code, but also for digital workspaces and assessment or certification information systems.

No 8	Requirement The digital services for education that support the school’s educational information system enable the exchange of school organisational data with other authorised digital services.

6.2.1. Scope of digital services for education

Providers of timetable and/or school life management solutions support the processes and activities based on the educational planning structure defined by the head teacher.

Chapter 4 of the digital technology doctrine for education describes the service for the exchange of educational planning data (Scope).

DRAFT

6.2.2. Interface between data providers and scope service providers

6.2.2.1. Standardised API exchanges

No 9	Requirement The various data and service providers that support educational institutions and schools in their teaching processes and activities enable communication based on standardised APIs, incorporating security measures that ensure user authentication, data integrity and the confidentiality of exchanges.

6.2.2.2. Scope Interface Contracts

No 10	Requirement Digital education services use the Scope platform to share data on educational organisation within the education sector.

A. Timetables (Scope Entry)

The single interface contract for the submission of educational planning data, between the Ministry of Education for the SCOPE service and each provider of timetable creation and management services, is available to authorised stakeholders in the Pléiade portal under[13] 'ESPACE ÉDITEURS INTERFACE ÉDUCATION NATIONALE' / 'emploi du temps'('NATIONAL EDUCATION INTERFACE PUBLISHERS' SPACE' / 'timetable').

B. Scope – Authorised Services Interface Agreement (Scope Exit)

The interface contracts between the MENJ Scope service and each stakeholder authorised to retrieve data from operational time uses will initially be available on an experimental basis in the form of APIs only. The Scope API will offer a range of services (available on request at osmose.coord-gen@ac-dijon.fr), each designed to address use cases agreed in advance with representatives of the management staff at EPLE.

[13] Publishers can apply to join by emailing communication-editeurs@education.gouv.fr

DRAFT

6.2.3. Standards

No 11	Requirement
	To facilitate the exchange of educational data, digital services for education rely on tried-and-tested standards such as EML (for email-style messages), iCal (for calendar invitations), vCard (for user contact details) and OneRoster (for course lists and associated data).

The table below sets out the applicable standards, along with their current status, within the scope of the educational organisation for school life.

Fields	Body	Standards	Comment	Status
Protocol / format	1EdTech	OneRoster	French profile coming soon, as part of ongoing work with 1EdTech. Data exchange elements for all school life data	Target
Format	IETF	EML	File format for electronic messages	Target
Format	Internet Mail Consortium	vCard	Address Book Format	Target
Format	IETF	iCal	Internet Calendaring and Scheduling Core Object Specification for the exchange and deployment of calendar and scheduling events.	Target

DRAFT

6.3. Digital service portals and digital resources and services for teaching and educational practices

Teachers' educational practices are supported by annual and periodic teaching programmes (progressions), facilitated by digital services of the 'homework diary' type for sequencing and organising the associated activities, as well as by digital educational resources providing content and tools for the benefit of teaching and learning.

No 12	Requirement Digital services for education that provide digital resources and services for teaching and educational practices organise their content according to a standardised semantic description and enable the integration of content units to facilitate the reuse of content or assessment modules, to report on learning experiences, or to monitor pupils' activity on an ongoing basis.

6.3.1. Providers of digital resources and services for teaching and educational practices

Teaching activities and educational practices are supported by a wide range of digital resources and services, which teachers select in accordance with their freedom of choice as teachers, exercised within the framework of their school or institution, which themselves benefit from regional digital resource and service initiatives.

Given the diversity of regional projects and the service providers involved, it is essential to establish common principles that enable educational tools and resources to be found, accessed, edited and integrated seamlessly across different services or service portals, whilst ensuring the protection of the personal data of pupils and education staff.

The main document setting out the reference frameworks of the digital technology doctrine for education describes the SDET framework for digital learning environments (ENTs), the CARMO framework for individual device projects, the CARINE framework for infrastructure services, and the GAR service for managing access to resources.

6.3.2. Requirements for data providers and service providers in the scope

6.3.2.1. Populating regional digital service portals

No 12 bis	Requirement Digital service portals run by regional projects populate their databases using the Ministry's information system, in accordance with data-feeding processes defined and overseen by the central directory.

DRAFT

Currently, the federated directory provides export files for ENT and mobile device projects.

6.3.2.2. Integration of content into education paths

No 13	Requirement Digital services for education must enable users to: - build an education path with pedagogical resources; - use educational modules within an education path without leaving it; - monitor the pupil's progress throughout their education path.

6.3.2.3. Portability and reversibility

No 14	Requirement Digital services for education must enable users to: - create sustainable and reusable pathways, thus independent of the different stakeholders; - export and import learning modules or education paths.

6.3.2.4. Exchanging personal data – GAR interface agreement

No 15	Requirement Digital services for education use the Core Services for Resource Access Management (GAR).

The GAR ensures authorisation control by linking user data with resource data

The interface contracts governing connection to the GAR are provided by the GAR's technical, functional and safety reference framework (RTFS). This is aimed at partners, resource providers on the one hand, and digital learning environment projects on the other. It is divided into three booklets and a package:

- 'General Presentation' booklet;
- 'Legal and administrative framework' booklet;
- 'Technical reference' booklet;
- packaging of supporting documents and examples.

The RTFS includes a version for identity providers, including ENT projects and their operators, and a version for resource providers.

The RTFS incorporates the interface contract of the ENT operators or resource providers.

DRAFT

It is available upon request at the address dne-gar(arobase)education.gouv.fr or on the GAR website, from the point of connection request.

6.3.3. Standards

No 16

Requirement

To meet the requirements of content integration, portability and reversibility, digital services for education rely on standard and proven protocols such as xAPI or LTI.

Standards that can be used for teaching with their status

Fields	Body	Standard	Comments.	Status
Track a pupil's progress throughout a course (learning records)				
Event/Protocol data	ADIL/IEEE	xAPI	Tin Can/xAPI is a configurable standard that can be used in all contexts (digital services, learning platforms, digital resources, formative and summative assessments, peer-to-peer interactions) to collect event data that provides a step-by-step account of a student's learning journey, as well as how a platform, service or resource is used.	Target
Event/Protocol data	1EdTech	Caliper Analytics	The Caliper standard provides a standardised and widely adopted framework for the collection and analysis of learning-related event data, thereby promoting a better understanding of pupils' activity throughout their educational journey.	Target
Exporting and importing learning modules or education paths				
Content Definition Metadata / Data Logic Model and Serialization	1EdTech	Common Cartridge	A content packaging standard for sharing content and education paths.	Target
Data for content conditioning and integration/Logical data model and serialisation	ADL/IEEE	Scorm	A format for developing and publishing reusable digital learning resources in learning management systems and other learning environments.	End of life

DRAFT

Using educational modules in an education path				
Data for content conditioning and integration/Logical data model and serialisation	H5P group	H5P	H5P is a plugin for existing publishing platforms that allows users to create interactive content such as interactive videos, presentations, games, quizzes and much more.	Target
Data for packaging and content integration	1EdTech	QTI	Format for exchange of test questions and structures, rating information	Target
Data for packaging and content integration/Protocol	1EdTech	LTI	A protocol allowing a learning management system to integrate personalised learning tools or experiences offered by another system.	Target
Describe educational resources				
Content definitions metadata/Data dictionaries, logical data model and serialisation	IEEE / AFNOR	ScoLOMFR	Description of resources.	Target

6.4. Exams, certifications and competitions

The table below shows the standards that can be used and their status for examinations, certifications and competitions.

Fields	Body	Standard	Comment	Status
Data model	European Commission	European Learning Model (ELM)	Multilingual data model for the interoperability of learning opportunities, qualifications, accreditation and skills credentials in Europe.	Target
Data model	1EdTech	Open Badge	Method for aggregating information on a single recognition or achievement, such as a micro-credential, skill, competence or diploma.	Target

DRAFT

6.5 Management of educational missions

6.5.1. Data and service providers for the evaluation of digital services for education

The management of educational missions falls under different levels of decision-making, from the institution or school up to the departments of the Ministry responsible for National Education, via the académies and local and regional authorities.

Assessment system are used to provide additional steering support for each of these decision-making levels, in order to support the steering of public education policy and digital service projects for education in particular.

6.5.2. Requirements for providers of digital resources and services for education

6.5.2.1. Use of standardised usage indicators

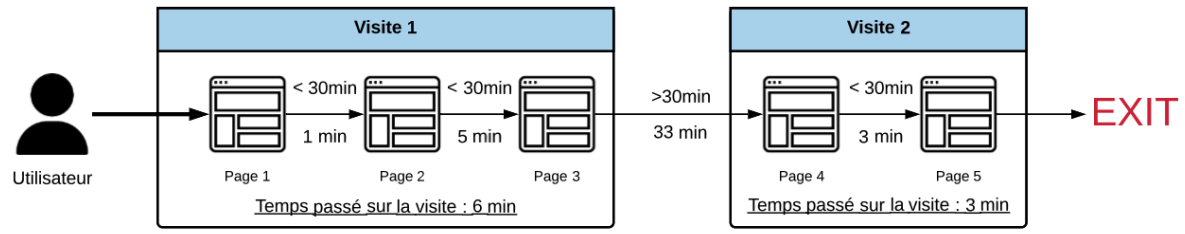
The number of visits is the standard metric used in web analytics tools. It refers to the viewing of pages on a website. As the use of digital services for education generally requires authentication, each visit is carried out by a user.

NO 17	Requirement To meet the needs of managing digital projects and policies, digital services for education are are able to provide at the very least two key indicators: visits and users.

If a user remains inactive for more than thirty minutes before resuming their activity, this counts as two visits. If the visitor is inactive for less than thirty minutes, it counts as just one visit.

If two users connect from the same computer (or other device), they each generate a visit and are considered different.

DRAFT



Visite 1 : temps passé sur la visite : 6mn
Visite 2 : temps passé sur la visite : 3mn

Visit 1: time spent on the visit: 6mn
Visit 2: time spent on the visit: 3mn

6.5.2.2. Integration into DNMA – audience measurement system

The DNMA is defined as a core service in Chapter 4 of the reference frameworks of the digital technology doctrine for education.

Digital learning environment (DLE) services that form part of the DNMA benefit from the standardised framework adopted for this scheme. The definition of the indicators produced by this system is the one adopted by the ACPM (Alliance for Press and Media Figures), and the tool used to collect these indicators is certified by this French professional association.

The DNMA is based on an external 'tagging' solution in line with a shared specification that defines the content and structure of the markers. The specification consists of:

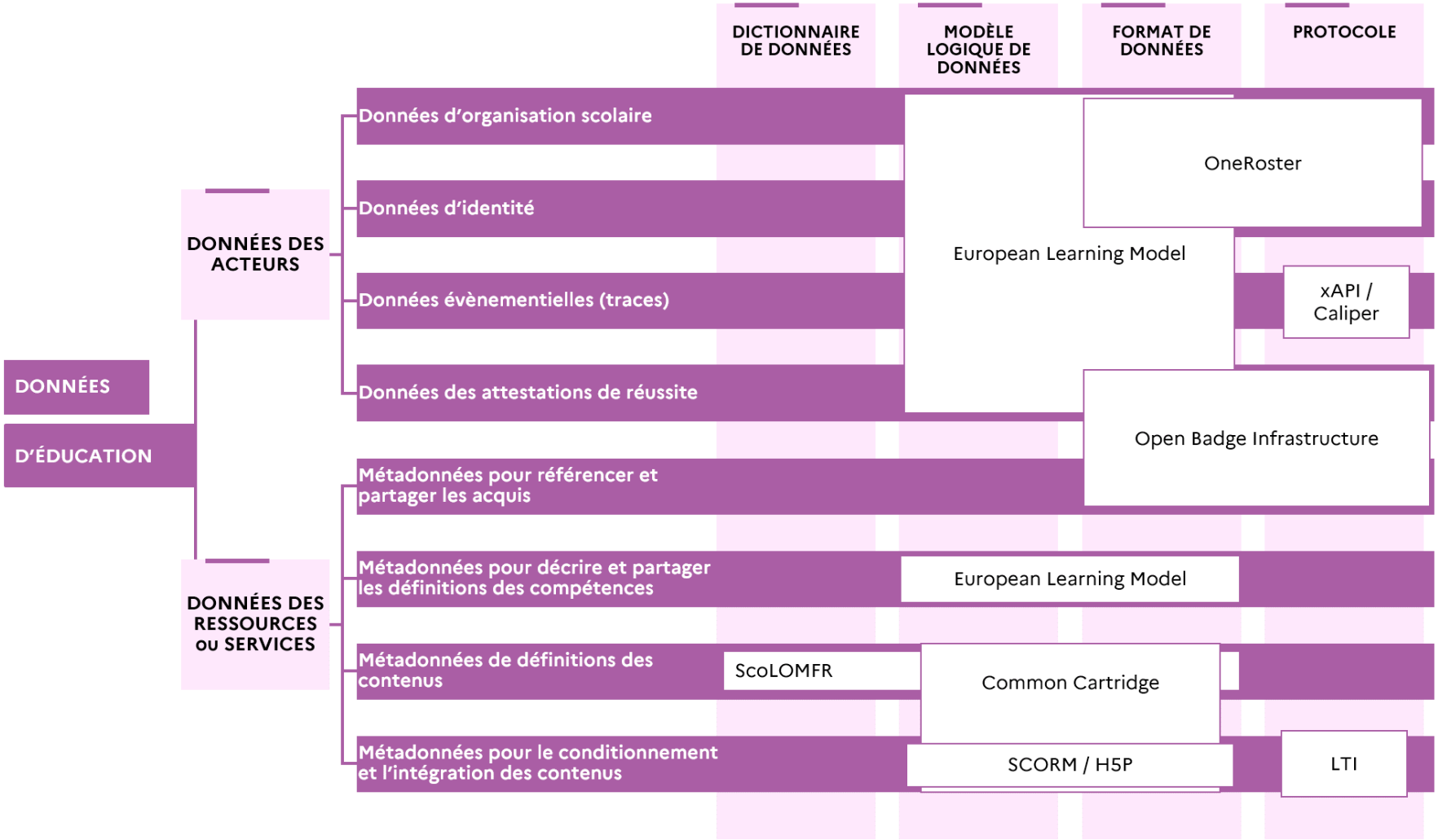
- the functional and technical integration reference framework (RFTI):
  - a description of the indicators used,
  - a reference list of service and tool indicators,
  - the technical and functional information required for the implementation of the DNMA marker,
  - a description of the requirements for compliance with the DNMA,
  - description of the complementary implementation options;
- of the marking plan:
  - it is the correlation table between the pages and functionalities of the ENT platform and the device's service repository, which makes it possible to interpret the device's statistics;
  - the labelling scheme is specific to each digital learning platform;
  - compliance with the marking plan is a DNMA compliance requirement.

6.5.3. Standards for measuring usage

No 18	Requirement
	To meet management needs and provide standardised usage metrics, digital resources and services for education are based on indicators set out in the DNMA.

DRAFT

7. Summary of the selected standards



DONNEES D'EDUCATION
DONNEES ACTEURS
DONNEES DES RESSOURCES OU SERVICE
DICTIONNAIRE DE DONNEES
MODELE LOGIQUE DES DONNEES

EDUCATION DATA
DATA ON STAKEHOLDERS
RESOURCE OR SERVICE DATA
DATA DICTIONARY
DIGITAL DATA MODEL

FORMAT DE DONNEES	DATA FORMATTING
PROTOCOLE	PROTOCOL
Données d'organisation scolaire	School organisation data
Données d'identité	Identity data
Données évènementielles (traces	Event data (traces)
Données des attestations de réussite	Data on certificates (of results)
Métadonnées pour référence et partager les acquis	Metadata for reference and for sharing achievements
Métadonnées pour décrire et partager les définitions des compétences	Metadata for describing and sharing competence definitions
Métadonnées de définitions des contenus	Metadata on content definitions
Métadonnées pour le conditionnement et l'intégration des contenus	Metadata for preparing and integrating content

Figure 7: Summary of the selected standards

DRAFT

Fields	Body	Standards	Comment	Status
Protocol	IETF	HTTPS	HyperText Transfer Protocol Secure: a combination of HTTP and a TLS encryption layer.	Target
Protocol		REST	Representational state transfer Software architecture style defining a set of constraints to be used to create web services.	Target
Format	IETF	JSON	JavaScript Object Notation. A text-based data format derived from the notation used for JavaScript objects.	Target
Format	W3C	XML	Extensible Markup Language. The initial objective of XML is to facilitate the automated exchange of complex content between heterogeneous information systems.	In use
Protocol	OIDF	Open ID Connect (OIDC)	Identification layer based on OAuth 2.0, authorisation device.	Target
Protocol	Internet engineering task force (IETF)	OAuth2	Authorisation protocol. Included in OIDC.	Target
Protocol	Organization for the Advancement of Structured Information Standards (OASIS)	SAML 2.0	Used by the GAR. Enables the exchange of authentication and authorisation data between security domains.	In use
Protocol	APEREO	CAS	Central Authentication Service. Support for OIDC, OAuth2 and SAML	End of life
Protocol / format	1EdTech	OneRoster	French profile coming soon, as part of ongoing work with 1EdTech.	Target

			Data exchange components for all school-related data.	
Format	IETF	EML	File format for electronic messages.	Target
Format	Internet Mail Consortium	vCard	Address Book Format.	Target
Format	IETF	iCal	Internet Calendaring and Scheduling Core Object Specification for the exchange and deployment of calendar and scheduling events.	Target
Event/Protocol data	ADIL/IEEE	xAPI	A protocol for reporting and tracking the traces left by activities.	Target
Event/Protocol data	1EdTech	Caliper Analytics	The Caliper standard provides a standardised and widely adopted framework for the collection and analysis of learning-related event data, thereby promoting a better understanding of pupils' activity throughout their educational journey.	Target
Content Definition Metadata / Data Logic Model and Serialization	1EdTech	Common Cartridge	A content packaging standard for sharing content and education paths.	Target
Data for content conditioning and integration/Logical data model and serialisation	ADL/IEEE	Scorm	Format for developing and publishing reusable digital learning resources to be used in learning management systems and other learning environments.	End of life
Data for content conditioning and integration/Logical data model and serialisation	H5P group	H5P	H5P is a plugin for existing publishing systems that allows users to create interactive content such as interactive videos, presentations, games, quizzes and much more.	Target
Data for packaging and content integration	1EdTech	QTI	Format for exchange of test questions and structures, rating information	Target

DRAFT

Data for packaging and content integration/Protocol	1EdTech	LTI	A protocol allowing a learning management system to integrate personalised learning tools or experiences offered by another system.	Target
Content definitions metadata/Data dictionaries, logical data model and serialisation	IEEE	ScoLOMFR	Description of resources.	Target
Data model	European Commission	European Learning Model (ELM)	Multilingual data model for the interoperability of learning opportunities, qualifications, accreditation and skills credentials in Europe.	Target
Data model	1EdTech	Open Badge	Method for aggregating information on a single recognition or achievement, such as a micro-credential, skill, competence or diploma.	Target

DRAFT

8. Use case

8.1. Access an educational resource

Description

A student wants to access a digital resource from their education path.

Example of an access scenario via GAR

- The student logs in to their school’s digital platform (ENT/OVS/LMS) via ÉduConnect
- As part of their education path, pupils access a digital resource (via a deep link)
- A learning session is opened on the resource provider via the student’s browser

Assumptions

- Responsibilities relating to access to and use of resources are governed by the GAR/GDPR contract
- The resource provider is accessible via a GAR URL
- The single authentication (SSO) carried out by the pupil via ÉduConnect allows the GAR to identify the pupil
- Resource allows granular access
- No proprietary tool used for content visualisation

DRAFT

Standards affected by this use case

Source	Destination	Transport protocol	Exchange standard	Interface specification	Description
ENT/OVS/LMS	ÉduConnect	HTTPS-REST	OIDC	ÉduConnect	Student identity provided by ÉduConnect after authentication
GAR	ENT/OVS/LMS	HTTPS	LTI	GAR	Access to the resource is via a GAR URL. The latter relays access to the resource provider after an authorisation check
ENT/OVS/LMS	Resource Provider	HTTPS	LTI	To be defined	Establishing an LTI session between the student's browser and the resource provider's server
ENT/OVS/LMS	ENT/OVS/LMS	REST	xAPI	To be defined	Record learning progress

8.2. Facilitate the integration of resources into an LMS for seamless use in an education path

Description

A teacher wishes to create a teaching path based on digital resources provided by several third-party publishers.

Example of an access scenario via GAR

- The teacher logs in to their school's digital platform (ENT/OVS/LMS).
- They design their education path using a list of accessible resources compiled by the GAR in the media centre provided by the digital services department

Assumptions

- The GAR is the provider of resource metadata

DRAFT

- The GAR verifies the identity of the teacher logged into its digital platform
- The list of resources compiled by the GAR is accessible to both the teacher and the pupils for whom the education path is intended
- The ENT is the provider of the user ID for the GAR.

Technical specifications and standards

Source	Destination	Protocol	Standard	Interface specification	Description
Agents Portal	ENT/OVS/ LMS	REST	OpenID Connect	Agents Portal	Authentication and identification of the teacher
GAR	ENT/OVS/ LMS	REST	ScoLOMFR	GAR	Provision of the list of resources accessible to the teacher

8.3 Ensure portability of the content of an education path when changing LMS

Description:

A teacher or member of the management team wishes, as part of a change of school, to transfer and import their data from the digital system at their previous school to the digital system at their new school.

Example of a scenario carried out on the digital learning platform of the sending school

- The teacher/PERDIR (personnels de direction - management staff) logs in to their home school's digital learning platform and submits a request to change schools and have their file transferred to their new school. They then select a list of the contents to be transferred.
- The sending digital learning environment sends a request to the receiving digital learning environment, including a list of content (homework diary, messaging, Moodle courses, teaching resources, etc.) and their source formats.
- The receiving digital learning environment analyses the request and responds with a list of compatible content types and formats.

Example of a scenario carried out on the digital learning platform of the receiving school

- The teacher/PERDIR logs in to the digital learning platform of their new school
- The digital learning platform automatically downloads and integrates data in a format compatible with the digital learning platform used by the receiving school.

DRAFT

- The teacher/PERDIR manually downloads content that is not compatible with the digital learning environment at the receiving school. The operation is carried out via the digital learning platform's user interface at the receiving school

Assumptions:

- The sending and receiving digital learning environments are able to verify the identity of the teacher or PERDIR requesting the transfer.

Source	Destination	Transport protocol	Exchange standard	Interface specification	Description
Agents Portal	ENT1 (departure) / ENT2 (arrival)	REST	OpenID Connect	Agents Portal: +link	Provision of teacher identity data
ENT1 (departure)	ENT2 (arrival)	REST	JSON	Single interface contract for ENT: +link	List of contents with their local formats
ENT2 (arrival)	ENT1 (departure)	REST	JSON	Single interface contract for ENT: +link	List of contents with compatible formats
ENT1 (departure)	ENT2 (arrival)	REST / S3	Binary, ScoLOMFR, Schema.org	Single interface contract for ENT: +link	Downloading binary content, or content formatted as ScoLOMFR/Schema.org index lists

DRAFT

ANNEX 3: Reference Framework for Responsible Digital Technology in Education

Table of contents

1. Preamble....60
   1.1. Context and objectives of the document....60
   1.2. Document life cycle and governance....60
2. Social and environmental responsibility....62
   2.1. Definition....62
   2.2. General principles of eco-design....62
   2.3. Reference texts and tools....62
   2.4. Eco-design levels....64
   2.5. Requirements for digital services for education....65
3. Digital accessibility....67
   3.1. Definition and scope....67
   3.2. General principles of accessibility....67
   3.3. Reference texts and tools....67
   3.4. Penalties....68
   3.5. Key considerations for accessibility....68
   3.6. Requirements for digital services for education....70
4. Data uses and protection of staff and users....71
   4.1. Definition....71
   4.2. Legal basis....71
   4.3. Digital identity of pupils....72
      4.3.1. Definitions....72
      4.3.2. General principles....72
      4.3.3. Requirements for digital services for education....72
   4.4. Right to disconnect....73
      4.4.1. Definitions....73
      4.4.2. General principles....73
      4.4.3. Requirements for digital services for education....74
5. Uses of AI and digital services for education....74
   5.1. Definitions....74
   5.2. Legal basis....75
   5.3. General principles....75
   5.4. Requirements for digital services for education....76

DRAFT

1. Preamble

1.1. Context and objectives of the document

This document serves as the reference framework for responsible digital technology in education. It forms part of the body of the reference frameworks of the digital technology doctrine for education, and of the digital strategy for education, which underscores the Ministry's ambition to foster citizenship in the digital age, as well as the necessary commitment of every digital service provider to work towards a shared goal of sustainable development.

It sets out the requirements and recommendations regarding environmental responsibility, digital accessibility, ethics and the use of AI for all providers of digital services for education.

It draws on general reference documents such as the RGESN and the RGAA, as well as the report by the commission entitled 'Screens and Children: In Search of Lost Time', and contextualises the requirements within the scope of digital services for education. The Ministry, its service providers and all partners and stakeholders in the digital services sector were involved in drawing up this framework.

Within the framework of this framework, it is understood that 'responsible digitalisation' is a process of continuous improvement aimed at reducing the environmental and social footprint of digital technology[14]. From an environmental perspective, it advocates a more restrained and energy-efficient use of digital technology by steering practices, usage patterns and deployment plans for equipment and services towards greater efficiency.

Socially responsible digitalisation aims to ensure digital inclusion, fair access to technology and the protection of human rights. This includes the fight against the digital divide and the promotion of digital ethics.

From an economic perspective, responsible digital promotes sustainable business models, financial transparency and ethical job creation. It is about promoting a digital economy that contributes positively to overall economic well-being.

1.2. Document life cycle and governance

The Ministry and its decentralised departments, local and regional authorities and industry stakeholders, as well as representatives of staff, pupils and families, are involved in the development of this framework. All stakeholders participate in the governance of the doctrine and its referentials through the consultation bodies.

---

[14] What is responsible digital technology? ? https://ecoresponsable.numerique.gouv.fr/publications/guide-pratique-achats-numeriques-responsables/demarche-numerique-responsable/definition/

DRAFT

This document is the third version of the reference framework for responsible digital technology in education.

An annual review, involving all relevant stakeholders, including staff and user representatives, enables an assessment of whether the document requires updating. The latter is then submitted to the Higher Council for Education (CSE) for its opinion.

DRAFT

2. Social and environmental responsibility

2.1. Definition

As part of a policy of restraint, the use of digital tools must always be assessed from a social and environmental perspective. We should therefore avoid digital solutions if there are alternatives that are less costly in environmental and social terms.

The social and environmental responsibility of a digital educational service involves incorporating environmental and social considerations into all development processes, with a view to reducing the environmental and social impacts of the digital service throughout its life cycle[15].

2.2. General principles of eco-design

The earlier environmental aspects are taken into account in the life cycle of the digital service (before, during or after its development), the greater the impact.

The integration of some basic principles should make it possible to reduce the consumption of computing and energy resources from terminals, networks and data repositories:

- simplicity of functionalities;
- the frugality and simplicity of the application architecture;
- relevance, i.e.: usefulness / response time / accessibility;
- sustainability, in particular by promoting the reuse and openness of software building blocks, as well as the use of APIs to facilitate data exchange.

Planning the use of data by the digital department, in accordance with the FAIR principles (Findable, Accessible, Interoperable, Reusable), is a key component of the process[16].

In order to address the challenges outlined above effectively, it is necessary to examine the official recommendations and, at the same time, to implement appropriate methods and tools.

DRAFT

[15] Luc, N. (30 January 2023). Eco-design of products. Ministries: Environment, Energy and Regional Affairs. https://www.ecologie.gouv.fr/leco-conception-des-produits

[16] Pasteur, C.-. I. (2023, August 2). FAIR principles: findable, accessible, interoperable, reusable. Open science: evolutions, challenges and practices. https://openscience.pasteur.fr/2020/10/05/les-principes-fair-findable-accessible-interoperable-reusable/

2.3. Reference texts and tools

[17]The General Ecodesign Framework for Digital Services (RGESN)

It was developed by **Arcep** and **Arcom**, in collaboration with **ADEME**, **DINUM**, **CNIL** and **Inria**. This document draws in particular on the previous work of the Interministerial Task Force on Environmentally Responsible Digital Technology (MiNumEco), led by DINUM and ADEME in collaboration with the Ministry for Ecological Transition and the Institute for Responsible Digital Technology (RGESN November 2022).

Report on software obsolescence by the General Council for the Economy[18]

It lists the various national and European texts on ecodesign and software obsolescence. It enables them to be consulted by functionality (planned obsolescence, extended software update provision, separation of corrective/evolutionary updates, etc.).

[19]Eco-responsible Digital Toolkit

A toolkit is available on the MiNumÉco website. It offers a (non-exhaustive) selection of software (both free and open-source) dedicated to the environmental impacts of digital technology.

This toolkit enables users to carry out a self-assessment of the eco-design process for a digital service, based on the 79 criteria of the RGESN.

DRAFT

[17] https://www.arcep.fr/mes-demarches-et-services/entreprises/fiches-pratiques/referentiel-general-ecoconception-services-numeriques.html

[18] https://www.economie.gouv.fr/cge/obsolescence-logicielle

[19] https://ecoresponsable.numerique.gouv.fr/publications/boite-outils/

2.4. Eco-design levels

As set out in the RGESN, various key areas must be taken into account when adopting an eco-design approach to digital services for education:

FRONTEND	FRONTEND
Limiter le poids et le nombre des requêtes par écran	To limit request weight and number per screen
Technique de mise en cache, de compression et de chargement progressif des contenus transférés	Features for caching, compressing and progressive loading of transferred content
Restreindre l'usage des capteurs des terminaux utilisateur	To restrict sensor use on user terminals
Héberger les ressources statiques sur un même domaine	To host static resources on the same domain
BACKEND	BACKEND
Configuration pour transmission de contenus compressés	Configuration for transferring compressed content
Date d'expiration des données et suppression en fonction	Expiry date of data and subsequent removal
Archivage de données	Data archiving
Système de cache pour les données plus utilisées	Cache system for the most-used data
Information sur les traitements en l'arrière-plan	Information on background processing
HEBERGEMENT	HOSTING
Choix hébergeur, « vert », engagé	Host choice, 'green', committed
Duplication de données / redondance du service	Duplication of data / redundancy of service
Hébergeur communique PUE et WUE	Host PUE and WUE notifications
Localisation géographique de l'hébergeur en cohérence avec celle de l'utilisateur	Alignment of host and user's geographic localisation
STRATEGIE	STRATEGY
Utilité / besoin & cibles utilisatrices	Usefulness / needs & user targets
Profils matériel utilisables	Usable material profiles
Utilisation technologies standards	Use of standard technologies
Dynamique de suivi : indicateurs & objectifs de réduction impacts environnementaux	Follow-up features: reduction of environmental impact (indicators & goals)
Référant en écoconception numérique	Digital eco-design plan
Déclaration et revues d'écoconception	Eco-design statement and reviews
Référentiel général d'écoconception de services numériques (RGESN)	General framework for the eco-design of digital services [RGESN]
CONTENU	CONTENT
Image / Vidéo / Audio / Document : Formats de fichiers & niveaux de compression adaptés	File formats & adapted compression levels, for images / video / audio / documents
Stratégie d'archivage et de suppression des contenus obsolètes	Archiving strategy and deletion of obsolete content
UX / UI	UX / UI
Service léger, utilisable en connexion bas débit	Light service, usable on low-speed connectionst
Animations, vidéos, sons : limités, sans lecture auto	Limited animations, videos, audio, without auto playback
Défilement de page fini, mettre en pause animations	End of page scrolling, animation pausing
Parcours navigation optimisé, informer du transfert	Optimised clickstream, to communicate transfers
Limiter le poids, les requêtes	Request weight limitation
Responsabilisation / moyens de contrôle pour l'utilisateur	Responsabilisation / user means of control
SPECIFICATIONS	SPECIFICATIONS
Revues de conception / de code avec un objectif de minimisation des impacts environnementaux	Design / code reviews to minimise environmental impacts
Stratégie de décommissionnement	Decommissioning strategy
Fournisseurs engagés également	Equally committed suppliers
Prendre en compte l'impact des composants d'interface prêt à l'emploi et des services tiers	Inclusion of the impact of ready-to-use interface components and third-party services
ARCHITECTURE	ARCHITECTURE
Architecture des ressources et composants pour réduire	Resource and component architecture to reduce

DRAFT

leurs impacts	their impact
Choix protocole d'échange	Exhange protocol options
Choix technologie	Technology options
Mises à jour correctives	Corrective updates

2.5. Requirements for digital services for education

In addition to the general framework outlined in the preceding paragraphs, the list below sets out the criteria required to integrate eco-design measures into the digital education sector in a practical and coordinated manner. This list is subject to change and has been agreed in consultation with the project leaders.

NO 1	Requirement Actions to develop digital services for education must comply with an ecodesign process that incorporates environmental constraints and the recommendations of the RGESN.

No 2	Requirement Each educational digital service provider shall publish an ecodesign declaration.

DRAFT

3. Digital accessibility

3.1. Definition and scope

Digital accessibility is about making digital content and services understandable and usable by people with disabilities.

3.2. General principles of accessibility

Since 2012, all public sites must be accessible and comply with all the criteria of the General Accessibility Improvement Framework (RGAA)[20] in order to allow all users equal access to their rights, in addition to an offer of non-digital services, necessary for the inclusion of all users.

3.3. Reference texts and tools

Digital public services and certain private services have an obligation to be equally accessible to all citizens, whether or not they have a disability. An accessible digital service is easier to use for people with disabilities and of better quality for all[21].

To facilitate the accessibility of digital websites and services, the Interministerial Directorate for Digital Affairs (Dinum) has published the he General Accessibility Improvement Framework. It contributes to the implementation of Article 47 of Law [22]No 2005-102 of 11 February 2005 on equal rights and opportunities, participation and citizenship of persons with disabilities and its[23] implementing decree No 2019-768 of 24 July 2019 on the accessibility of online communication services to the public for persons with disabilities.

The technical component of the RGAA is a method of application of the international standard (an international standard issued by the W3C (World Wide Web Consortium)): WCAG 2.1[24]; a European standard issued by the ETSI (European Telecommunications Standards Institute): EN 301 549 v3.2.1 (March 2021)[25]).

To ensure that a digital service complies with the RGAA, the following elements must be provided for each online service:

- The **accessibility declaration** which must contain the following information:

[20] https://accessibilite.numerique.gouv.fr/

[21] https://accessibilite.numerique.gouv.fr/methode/criteres-et-tests/

[22] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000809647

[23] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038811937

[24] https://www.w3.org/TR/WCAG21/

[25] https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32021D1339

DRAFT

a compliance status;

notification of non-accessible content;

assistive and contact mechanisms;

a reference to the right of the person concerned to refer the matter to the Ombudsman.

- Display the RGAA compliance rate for the site or service on **all pages**:

  'Accessibility: non-compliant', if no audit has been carried out or if the result is less than 50 %;

  'Accessibility: partially compliant' if the audit result is higher than 50 %;

  'Accessibility: fully compliant' if the score is 100%.

- Each online service shall provide a link to its multi-annual scheme, lasting up to three years, outlining the respective entity's digital accessibility policy. The multi-year accessibility plan sets out how accessibility is implemented within an organisation; this is generally carried out in four stages:
  - assessment: identification of services and assessment of their level of accessibility;
  - logging: production of one accessibility statement per service;
  - organisation: establishing a structure to improve services and drawing up annual action plans;
  - communication of these elements on the organisation's website.

- This applies to all websites and apps accessed via a web browser:
  - websites, intranets, extranets and software packages;
  - mobile applications;
  - 'digital furniture'.

The RGAA is regularly subject to new versions and updates to adapt to web developments but also to changes in standards and regulations.

3.4. Penalties

Failure to comply with the reporting obligations described above may result in a financial penalty issued by ARCOM[26].

Where breaches are identified by authorised officers, Arcom may issue a formal notice to the legal entities responsible for the service, requiring them to comply with the relevant legal provisions. If they continue to fail to comply with the law, the Authority may impose

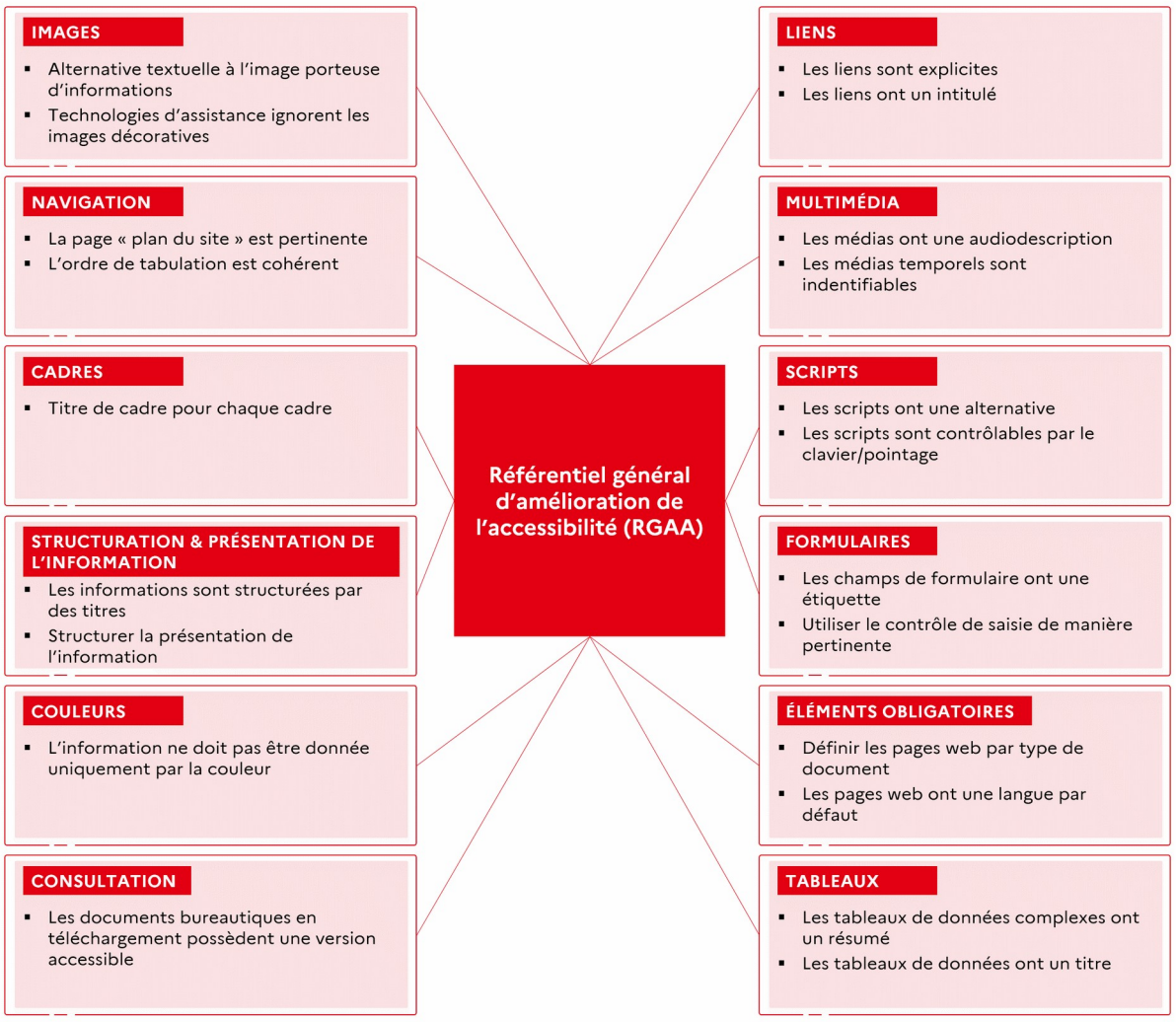
[26] Source: https://www.arcom.fr/nous-connaitre/nos-missions/garantir-le-pluralisme-et-la-cohesion-sociale/les-droits-des-personnes-handicapees/accessibilite-des-sites-et-des-services-numeriques

DRAFT

financial penalties on them, the level of which will be determined according to the nature, seriousness and duration of the breach.

3.5. Key considerations for accessibility

As set out in the RGAA, various aspects must be taken into account when implementing an accessibility process that takes into account the technical constraints and regulatory criteria that must be met.



IMAGES	GRAPHICS
Alternative textuelle à l'image porteuse d'informations Technologies d'assistance ignorent les images décoratives	Alternative text to the info graphic Assistive technologies overlook decorative graphics
NAVIGATION	NAVIGATION
La page « plan de site » est pertinente L'ordre de tabulation est cohérent	The site map page is relevant$ The tab order is coherent
CADRES	FRAMES
Titre de cadre pour chaque cadre	Frame title for each frame
STRUCTURATION & PRESENTATION DE L'INFORMATION	INFORMATION STRUCTURE & PRESENTATION
Les informations sont structurées par des titres Structurer la présentation de l'information	The information is structured by title To structure the presentation of information
COULEURS	COLOURS

L'information ne doit pas être donnée uniquement par la couleur	Information must not be given by the colour only
CONSULTATION	CONSULTATION
Les documents bureautiques en téléchargement possèdent une version accessible	There is an accessible version for downloadable automated office documents
Référentiel général d'amélioration de l'accessibilité (RGAA)	General Accessibility Improvement Framework [RGAA]
LIENS	LINKS
Les liens sont explicites Les liens ont un intitulé	The links are clear The links have no title
MULTIMEDIA	MULTIMEDIA
Les médias ont une audiodescription Les médias temporels sont identifiables	The media have an audio description Temporal media are identifiable
SCRIPTS	SCRIPTS
Les scripts ont une alternative Les scripts sont contrôlables par le clavier/pointage	The scripts have an alternative The scripts can be controlled by keyboard/pointing
FORMULAIRES	FORMS
Les champs de formulaire ont une étiquette Utiliser le contrôle de saisie de manière pertinente	The form fields are labelled To use the input control as relevant
ELEMENTS OBLIGATOIRES	OBLIGATORY ELEMENTS
Définir les pages web par type de document Les pages web ont une langue par défaut	To define the webpages by document type The webpages have a default language
TABLEAUX	TABLES
Les tableaux de données complexes ont un résumé Les tableaux de données ont un titre	The complex data tables have a summary The data tables have a title

3.6. Requirements for digital services for education

No 3	Requirement
	Digital services for education must be made accessible in accordance with the RGAA.

DRAFT

4. Data uses and protection of staff and users

4.1. Definition

Digital services raise ethical and legal questions relating to data, algorithms and their uses. The aim is to develop and support solutions that are consistent with the core values of education and with the existing legal framework.

This chapter sets out the shared principles that should guide the development and use of digital technologies in education, with a view to ensuring that digital technology serves the interests of users, and more specifically those of pupils.

The interoperability component of this doctrine also Also contributes to setting a standard to ensure the neutrality of the impact of technological choices and enable the operation of services and resources regardless of the technological choices made by the project promoters.

4.2. Legal basis

a) **Law of 7 July 2023** aimed at establishing a digital age of majority and combating online hatred.

This law sets the minimum age for signing up to social media at 15. Provisions to improve the prevention and prosecution of online offences, such as cyberbullying, are included in the legislation.

b) **Law of 21 May 2024** to secure and regulate the digital department, known as the 'SREN'

This law introduces a number of measures relating to anti-scam filters, the rapid blocking of pornographic websites accessible to children, and the banning of cyberbullies from social media, with a view to better regulating the digital space and protecting internet users, particularly the youngest among them. It also requires pornographic websites to verify the age of their users in order to protect children from online pornography.

c) The report **'Children and Screens In Search of Lost Time'**, presented to the President of the Republic in April 2024.[27]

This report, drawn up by a panel of experts, assessed the impact of children's screen time and put forward recommendations on how to ensure it is used appropriately.

d) **IGESR Report No 24-25 140C 'Digital technology in school-family relations'**[28]

This report assesses the impact of digital workspaces (ENT) and school management software on the relationship between schools and families. It makes recommendations to regulate its use and preserve the quality of this relationship.

[27] https://www.elysee.fr/admin/upload/default/0001/16/fbec6abe9d9cc1bff3043d87b9f7951e62779b09.pdf

[28] https://www.education.gouv.fr/usages-du-numerique-dans-la-relation-ecole-familles-450666

DRAFT

4.3. Digital identity of pupils

4.3.1. Definitions

An identity can generally be defined as ‘that which enables us to distinguish ourselves from others, without any possible ambiguity, in a given context’. The concept of context is very important for understanding the concept of identity, as it determines the population within which we wish to distinguish the individual.

For digital identity, depending on the context, more or less extensive dataset will therefore be necessary for the identification of an individual. And depending on the sensitivity of the service that the individual wishes to access, the service provider will require a more or less robust identity verification process.

Digital identity therefore refers to the association of a single identifier with specific attributes (surname, first name, date of birth, etc.) that can be exploited by various digital services. It is essential for the operation of individual access services.

Throughout their lives, each person has several digital identities, linked to their identity.

In an educational context, pupils’ digital identity refers to the specific credentials that enable them to access, on an individual basis, the various digital services provided to them by virtue of their affiliation with a school, a local education authority or a region, or even at national level. Individual access to digital services and resources generally requires *identification* (the unique verification of an entity – a user or device) and *authentication* (which supplements identification by providing proof of identity).

The student verifies their identity by linking the identification process to a personal, secret and revocable element (for example: a password, a key or a security code). This mechanism shall ensure appropriate access to personal online services and resources.

The ‘digital age of majority’ refers to the age at which a minor is legally considered capable of consenting independently to the use of their personal data online, in particular when signing up to social media platforms, without requiring the authorisation of a legal representative.

4.3.2. General principles

In order to protect pupils, particularly the youngest ones, from excessive exposure to screens and digital services, it is necessary to **limit their use** and to **support them in developing their digital identity**.

Digital services for education must therefore incorporate operational principles that respect educational objectives and teaching needs, taking into account the different levels or stages of education.

This version of the document addresses the specific requirements relating to ‘young pupils’ (particularly those in cycles 1 and 2) in the area of digital identity.

DRAFT

4.3.3. Requirements for digital services for education

	Requirement
No 4	When used with pupils in cycles 1 and 2, digital services and resources must not require individual authentication to complete an activity. Management of pupils' access to these resources may be carried out by the teacher by simply providing a classroom account, for example.

	Requirement
No 5	When used with pupils in cycles 1 and 2, digital services and resources are restricted to use in the classroom and under the supervision of a teacher. There is therefore no need for identification/authentication for independent activities at home.

	Requirement
No 6	In the case of digital educational resources offering personalised activities (e.g. adaptive learning pathways) or individually assessed activities, the use of authenticated access is not permitted for cycles 1 and 2. However, for cycle 2, a system of individual identification that allows each pupil access to this type of resource remains permitted, provided that its use is properly supervised by the teacher during school hours.

	Requirement
No 7	In cycle 2, learning progress can be tracked by identifying individual pupils. Authentication – to prove identity – must not be required by the service/resource to enable such tracking. Consequently, it is not possible for the pupil's academic record to be based on the automatic uploading of learning data.

4.4. Right to disconnect

4.4.1. Definitions

The right to disconnect has been enshrined in the Labour Code since 2017, in the workplace. This is a principle whereby an employee has the right not to be connected to work-related digital devices (mobile phones, emails, etc.) outside working hours.[29]

4.4.2. General principles

In line with the proposals of the 'Children and Screens' commission and the recommendations of the General Inspectorate of Education, Sport and Research (IGÉSR), a suspension of information updates has been introduced in the evenings and at

[29] Article L2242-8 of the Labour Code: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037389692/2018-09-07

DRAFT

weekends for all digital tools used to maintain links between schools, institutions, pupils and families (notably school life software and digital learning environments).

This provision means that these tools are set by default not to publish any new information or content between 8 pm and 7 am on weekdays, and from 8 pm on Friday to 7 am on Monday morning at the weekend. This applies to communication tools (messaging, blogs, chat rooms, etc.) as well as notes, homework and all school-related information.

School management staff retain the autonomy to fine-tune the implementation of this provision in line with the specific circumstances of their area, their institution and any emergency situations that may arise.

4.4.3. Requirements for digital services for education

Digital workspaces and school life suites already include certain features that allow for customisation at school level.

The implementation timeline for the technical doctrine's requirements will take account of the constraints publishers face in incorporating them into their annual product roadmaps.

No 8	Requirement Digital services that help connect schools, educational establishments, pupils and families (such as school life management systems and digital learning environments) are set by default to suspend the sending of new messages on weekdays between 8 pm and 7 am the following morning, and from 8 pm on Friday evenings until 7 am on Monday mornings at the weekend. Access to digital services remains available for viewing and data entry during the suspension period. Where applicable, the visibility granted to recipients regarding entries made during the relevant suspension period is deferred until the end of that period. To raise the sender's awareness, the digital services shall display a message reminding them of their right to disconnect.

No 9	Requirement Digital services that help connect schools, educational establishments, pupils and families (such as school life management suites and digital learning environments) offer configuration options to school management staff, enabling them to adapt the rules governing the right to disconnect to local circumstances, the specific needs of the school and the handling of emergency situations.

DRAFT

5. Uses of AI and digital services for education

5.1. Definitions

AI is defined as any digital service based on probabilistic algorithms, relying on the statistical processing of large datasets on which they are trained and capable of producing results comparable to those obtained by human cognitive activity.

The term 'predictive AI' is used to describe models that can classify data or anticipate events, trends or risks, while 'generative AI' refers to models capable of producing content (text, images, audio, video).

5.2. Legal basis

- Regulation (EU) No 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (known as the 'AI Regulation') of 13 June 2024[30];
- Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, adopted by the Council of Europe on 17 May 2024[31];
- Rules on the protection of personal data, in particular the GDPR, for AI systems or models involving the processing of personal data[32].

General recommendations on the use of artificial intelligence systems in the context of education are described in the 'Framework for the use of AI in education'.

The CNIL also provides useful guidance on the use of AI systems in schools.

5.3. General principles

The 'Framework for the use of AI in education' specifies the main principles to be respected:

- comply with the legal framework (in particular the GDPR and the AI Regulation)
- ensure the educational added value of the use of AI;
- ensure that data entered into the tools is protected and refrain from using consumer-grade generative AI where personal data is involved;
- be aware of the environmental impact of generative AI and refrain from using it if more environmentally friendly solutions are available to meet the need;
- demonstrate transparency in its use;
- think critically about the content produced.

[30] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202401689

[31] https://www.coe.int/fr/web/artificial-intelligence/la-convention-cadre-sur-l-intelligence-artificielle

[32] https://www.cnil.fr/fr/developpement-des-systemes-dia-les-recommandations-de-la-cnil-pour-respecter-le-rgpd

DRAFT

It also sets out specific guidelines for pupils: for example, the educational use of generative AI services in the classroom is permitted from Year 4 onwards and in line with UNESCO's recommendations. Generative AI services may be used independently in secondary schools within an educational framework explicitly defined by the teacher. Any use of generative AI to complete a school assignment, without the teacher's explicit permission and without the student having made an independent effort to understand the material, is considered cheating.

This framework is also part of a broader strategy to train teachers in computational thinking and AI, in both initial and continuing professional development.

5.4. Requirements for digital services for education

	Requirement
No 10	Digital services and resources for education must take into account the principles set out in the 'Framework for the Use of AI in Education[33]'.

	Requirement
No 11	Digital educational services and resources may incorporate generative AI tools for use by pupils in the classroom, provided that access is genuinely anonymised and secured via the GAR, from Year 4 onwards and under the supervision of a teacher, and independently from secondary school onwards within a framework defined by the teacher.

DRAFT

[33] https://www.education.gouv.fr/cadre-d-usage-de-l-ia-en-education-450647

ANNEX 4 - Conformity criteria by type of service concerned and associated application deadlines

			Time limit applicable in months from the date of publication of the order according to the type of service					
Theme	No	Conformity criteria	Services providing timetable functions	Services that provide the educational community of a school with access to teaching and learning resources (digital learning platforms, media centres, etc.)	Services providing educational content and/or educational services	Services providing infrastructure and equipment management functions	Services responsible for administrative management, formalities and procedures relating to the national education system, or support functions	Services supporting school life initiatives
Security	1	Ability to provide the documentary evidence needed to respond to the various security checks and audits defined by the project promoters or the relevant working group	10	10	10	10	10	10
Security	2	Ability to respond to security incidents and address project owners' requests	10	10	10	10	10	10
Security	3	Ability to deploy the necessary resources to meet the requirements of the Department's Operational Digital Security Policy (POSN)	10	10	10	10	10	10
Interoperability	4	Integration with ÉduConnect where identification and authentication of pupils and their guardians is required	N/A	10	N/A	34	34	10
Interoperability	5	Interfacing with Agent Portals where agent identification and authentication is required	22	22	N/A	22	22	22

DRAFT

Theme	No	Conformity criteria	Services providing timetable functions	Services that provide the educational community of a school with access to teaching and learning resources (digital learning platforms, media centres, etc.)	Services providing educational content and/or educational services	Services providing infrastructure and equipment management functions	Services responsible for administrative management, formalities and procedures relating to the national education system, or support functions	Services supporting school life initiatives
Interoperability	6	Ability to use APIs exposed by Scope output to consume educational planning data in compliance with the applicable Scope interface contract	N/A	10	34	34	N/A	10
Interoperability	7	Integration with Resource Access Manager (GAR)	N/A	10	10	N/A	N/A	22
Interoperability	8	Using the tagging tool of the National Audience Measurement System (DNMA)	N/A	10	N/A	N/A	N/A	22
Interoperability	9	The ability to provide, via the Scope service, for the purposes of operating digital learning environments (ENTs), in accordance with the current "Scope entry" interface contract, spatio-temporal data on the organisation of teaching, optional activities and support measures implemented within the institution	12	N/A	N/A	N/A	N/A	N/A

DRAFT

Theme	No	Conformity criteria	Services providing timetable functions	Services that provide the educational community of a school with access to teaching and learning resources (digital learning platforms, media centres, etc.)	Services providing educational content and/or educational services	Services providing infrastructure and equipment management functions	Services responsible for administrative management, formalities and procedures relating to the national education system, or support functions	Services supporting school life initiatives
Interoperability	10	The ability to provide, via the Scope service and in accordance with the Scope interface agreement that has come into force, data relating to groups and student-group relationships generated by any timetable solution	10	N/A	N/A	N/A	N/A	N/A
Interoperability	11	Ability to provide indicators of service traffic in accordance with those defined in the interoperability framework	N/A	10	22	N/A	34	22
Interoperability	12	Ability to provide the completed specific ENT conformity grid at the request of the project promoters	N/A	10	N/A	N/A	N/A	N/A
Interoperability	13	Compliance with the national education nomenclatures in force, including the Central Nomenclature Base (BCN)	10	10	10	10	10	10
Interoperability	14	Compliance with the open and documented interface standards set out in the interoperability framework for solutions that interface with education path design tools via the GAR or through integration	N/A	22	N/A	N/A	N/A	N/A

DRAFT

Theme	No	Conformity criteria	Services providing timetable functions	Services that provide the educational community of a school with access to teaching and learning resources (digital learning platforms, media centres, etc.)	Services providing educational content and/or educational services	Services providing infrastructure and equipment management functions	Services responsible for administrative management, formalities and procedures relating to the national education system, or support functions	Services supporting school life initiatives
Interoperability	15	Using exports from the Central Directory	N/A	10	N/A	10	N/A	10
Interoperability	16	Providing the user with an export function in an open and documented format, as specified in the interoperability framework, for their user data generated through the use of the service	10	10	10	N/A	10	10
Interoperability	17	Use of an open and documented format as referred to in the interoperability framework for the exchange and circulation of pedagogical organisation data	10	10	22	22	22	10
Interoperability	18	Compliance with open and documented protocols (as specified in the interoperability framework) for the identification and authentication of participants	10	10	10	10	10	10
Interoperability	19	Ability of resources to use standardised descriptions so that modules can be integrated	N/A	22	22	N/A	N/A	N/A

DRAFT

Theme	No	Conformity criteria	Services providing timetable functions	Services that provide the educational community of a school with access to teaching and learning resources (digital learning platforms, media centres, etc.)	Services providing educational content and/or educational services	Services providing infrastructure and equipment management functions	Services responsible for administrative management, formalities and procedures relating to the national education system, or support functions	Services supporting school life initiatives
Interoperability	20	The ability to provide users with tools for creating education paths or to integrate a third-party service that enables this	N/A	10	10	N/A	N/A	N/A
Interoperability	21	Use of an open and documented format specified in the interoperability framework when providing a feature to track a pupil's activity throughout their educational journey (event-based data known as 'learning traces')	N/A	22	22	N/A	N/A	N/A
Interoperability	22	Use of an open and documented format specified in the interoperability framework when using learning modules within a learning pathway, or	N/A	22	22	N/A	N/A	N/A

DRAFT

		when providing a feature for importing or exporting learning modules or education paths.						
Theme	No	Conformity criteria	Services providing timetable functions	Services that provide the educational community of a school with access to teaching and learning resources (digital learning platforms, media centres, etc.)	Services providing educational content and/or educational services	Services providing infrastructure and equipment management functions	Services responsible for administrative management, formalities and procedures relating to the national education system, or support functions	Services supporting school life initiatives
Interoperability	23	Providing users with an export function in an open and documented format, as specified in the interoperability framework, for their user data where data management features relating to examinations, skills certifications or competitive examinations are made available	N/A	10	10	N/A	10	10
Interoperability	24	Provision of user-oriented APIs to facilitate the real-time exchange of user-related information under authenticated conditions	10	N/A	N/A	N/A	N/A	10

DRAFT

Interoperability	25	Compliance with the recommendations of the reference framework for digital infrastructure services in schools and educational establishments (CARINE)	N/A	N/A	N/A	10	N/A	N/A
Interoperability	26	Compliance with the recommendations set out in the CARMO framework for accessing educational resources via mobile devices when planning a mobile device project	N/A	10	10	10	N/A	10

DRAFT

Theme	No	Conformity criteria	Services providing timetable functions	Services that provide the educational community of a school with access to teaching and learning resources (digital learning platforms, media centres, etc.)	Services providing educational content and/or educational services	Services providing infrastructure and equipment management functions	Services responsible for administrative management, formalities and procedures relating to the national education system, or support functions	Services supporting school life initiatives
Interoperability	27	The ability of the proposed resources to interface with other digital services in an open and documented format as described in the interoperability framework	N/A	N/A	10	N/A	N/A	N/A
Responsible Digital Technology	28	Incorporation into the eco-design processes for digital services set out in the General Framework for the Eco-design of Digital Services (RGESN)	34	34	34	34	34	34
Responsible Digital Technology	29	Publication of an eco-design declaration for digital services	34	34	34	34	34	34
Responsible Digital Technology	30	The ability to set a default configuration to suspend the distribution of new information on weekdays between 8 pm and 7 am the following morning, and at weekends from 8 pm on Friday evening to 7 am on Monday morning.	N/A	10	10	N/A	N/A	10
Responsible Digital Technology	31	Maintaining access to digital services, both for viewing and inputting data, during the daily and weekly suspension periods relating to the release of new information	N/A	10	10	N/A	N/A	10

DRAFT

Theme	No	Conformity criteria	Services providing timetable functions	Services that provide the educational community of a school with access to teaching and learning resources (digital learning platforms, media centres, etc.)	Services providing educational content and/or educational services	Services providing infrastructure and equipment management functions	Services responsible for administrative management, formalities and procedures relating to the national education system, or support functions	Services supporting school life initiatives
Responsible Digital Technology	32	Ability to provide delayed visibility to recipients in the case of entries made during the daily and weekly suspension periods relating to the dissemination of new information	N/A	10	10	N/A	N/A	10
Responsible Digital Technology	33	The ability to display a message reminding users of their right to disconnect during the daily and weekly blackout periods relating to the release of new information.	N/A	10	10	N/A	N/A	10
Responsible Digital Technology	34	The ability to provide management staff with configuration options enabling them to adapt the rules governing the right to disconnect in line with regional constraints, the specific needs of the organisation, and the handling of emergency situations.	N/A	10	N/A	N/A	N/A	10

DRAFT

Theme	No	Conformity criteria	Services providing timetable functions	Services that provide the educational community of a school with access to teaching and learning resources (digital learning platforms, media centres, etc.)	Services providing educational content and/or educational services	Services providing infrastructure and equipment management functions	Services responsible for administrative management, formalities and procedures relating to the national education system, or support functions	Services supporting school life initiatives
Responsible Digital Technology	35	Ability of the application offering functionalities based on artificial intelligence to take into account the 'framework for the use of AI in education'.	10	10	10	N/A	10	N/A
Responsible Digital Technology	36	Where generative AI-based features are proposed: the ability to implement teacher supervision for use in the classroom by pupils from Year 8 onwards, and a self-directed mode for pupils from secondary school onwards, within the framework defined by the teacher	10	10	10	N/A	10	N/A

DRAFT