# Children's data protection in an education setting

## Guidelines

Consultative committee of the convention
for the protection of individuals
with regard to automatic processing
of personal data

**Convention 108**

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

# Children's data protection in an educational setting

## Guidelines

Adopted by the Committee
of the Convention for the protection
of individuals with regard to automatic
processing of personal data
(Convention 108)

Council of Europe

French edition:
*La protection des données personnelles des enfants dans un cadre éducatif*



Cover and layout: Documents and Publications Production Department (SPDP), Council of Europe

Photos: Shutterstock


Printed at the Council of Europe

# Contents

# 1. Introduction

The digital environment shapes children's lives in many ways, creating opportunities for and risks to their well-being and enjoyment of human rights. Some digital tools enable the delivery of essential information, connecting school communities outside the classroom. Others provide ways to share educational content or offer vital alternative means and modes of education through assistive technology and enhanced communication.

These guidelines[1] should support organisations and individuals in the context of education to respect, protect and fulfil the data-protection rights of the child in the digital environment, within the scope of Article 3 of the modernised Convention 108 (more commonly referred to as "Convention 108+"),[2] and in accordance with the Council of Europe instruments including the Guidelines to respect, protect and fulfil the rights of the child in the digital environment Recommendation CM/Rec(2018)7.[3]

The UN Convention Committee on the Rights of the Child sets out in 2001 that:

> Children do not lose their human rights by virtue of passing through the school gates. Education must be provided in a way that respects the inherent dignity of the child and enables the child to express his or her views freely[4]

1. The guidelines follow and build on the report "Children's Data Protection in Education Systems: Challenges and Possible Remedies", drafted by Jen Persson, Director of defenddigitalme, available at https://rm.coe.int/t-pd-2019-06rev-eng-report-children-data-protection-in-educational-sys/168098d309.
2. Convention 108+: Convention for the protection of individuals with regard to the processing of personal data as modernised by the Amending Protocol CETS No. 223, available at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.
3. Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a.
4. UN Convention Committee on the Rights of the Child; General Comment no. 1 (2001) on Article 29 (1): The aims of Education; 17 April 2001; The Convention on the Rights of the Child (unicef-irc.org)

The introduction of digital tools to the classroom in effect opens up the school gates to a wide range and high volume of stakeholders who interact with children's everyday activities. The majority of the devices and applications, software and learning platforms adopted in educational settings are developed by private, commercial companies.

Stakeholders should collaborate to create a rights-respecting environment, to uphold Article 8 of the European Convention on Human Rights and protect the human dignity and fundamental freedoms of every individual, in respect of data protection.

Much commercial software in education is known as "freeware": software offered to educational settings at no direct financial cost. According to the European Union (EU) e-Commerce Directive (Article 1.1), this would generally fall within the definition of an Information Society Service[5] "provided for remuneration".

The expansion of educational technology can mean non-state actors routinely control children's educational records not only in independent schools but also in state schools. The digital infrastructure to deliver state education is often commercially owned. This can introduce new questions of where control of the curriculum sits if content type and delivery is shaped by the technology platform, as well as questions about security and sustainability.

Therefore, it can lie within the power of companies to lock in schools to proprietary software practices, and schools must be aware of the potential consequences for interoperability, for data access and reuse, and the budgetary and environmental impacts of obsolescence, for example where a company decides to discontinue hardware or software upgrades. It is common, at the time of writing, for small companies to be incubated by angel investors and later be bought out by other larger companies. Control and storage of personal data can thus be transferred in takeovers several times over in the course of a child's education.

The growth of cloud-based and transborder data flows in educational data systems means security practices require particular attention, in accordance with Article 7 of Convention 108+.

Children cannot see or understand how large their digital footprint has become or how far it travels to thousands of third parties across or beyond the education landscape throughout their lifetime. While children's agency is

5. To determine the scope of the term "information society service" in the GDPR, for example, reference is made in Article 4(25) of the GDPR to Directive 2015/1535. See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 (para 128).

vital and they must be better informed about how their own personal data are collected and processed, there is at the same time a consensus that children cannot be expected to understand a very complex online environment and to take on its responsibilities alone.

The investigative burden needed before procuring products or services in educational settings can make it hard even for adults to fully understand software tools and their processing, including assessing the comparative implications of using open or proprietary information and communication technology (ICT), paid-for-services or freeware or to carry out adequate risk assessment, and to retrieve and offer the relevant information required to provide to the data subject. This makes it hard to be sufficiently qualified to meet and uphold users' rights.

Recognising that legislation on educational settings and other domestic and international laws have an impact on how the data-protection rules are applied, including the rights of data subjects, educational institutions need strong legislative frameworks and codes of practice to empower staff, and to give clarity to companies to know what is permitted and what is not when processing children's data in the context of educational activities, creating a fair environment for everyone.

Policy makers and practitioners, including legislators, supervisory authorities in accordance with Article 15, paragraph 2.*e*, of Convention 108+, educational authorities and the industry should all follow and promote these guidelines and implement measures to meet data protection and privacy obligations.

In educational settings, children are disempowered in their relationship with a public authority and are also recognised as vulnerable due to their lack of understanding and evolving capacities and their state of being in the process of developing into adulthood. From a static point of view, the child is a person who has not yet attained physical and psychological maturity. From a dynamic point of view, the child is in the process of developing to become an adult.[6] Children are also active rights holders and agents who require not only protection but also provision of information, training and guidance.

Materials such as informational guides and fair processing documents should also be made available to children and their representatives, in a child-friendly and accessible manner.

6. Working Party 29 Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf.

The breadth of personal data that may be processed, their wide range of uses, including in support of learning and non-learning aims, for administration, behavioural management and teaching purposes, their sensitivity and the lifelong risks to privacy that may arise from processing both non-digitised and digitised records in an educational setting should be recognised.

These guidelines should also apply wherever remote e-learning solutions and services are engaged as the result of a child's enrolment in an educational setting and are used outside the educational school, such as for homework or distance learning. Distance-learning tools and resources should be subject to the same rigorous due diligence for pedagogical quality, safety and data-protection standards, for instance regarding the default settings, so that the usage of applications and software does not infringe the rights of the data subjects (data protection by default). Processing must not involve more data than necessary to achieve the legitimate purpose. This is particularly important when consent cannot be freely given because the choice is to use a product and receive remote instruction or refuse and receive none.

When a school requires the use of e-learning tools, a consent basis for processing personal data either by the school or by the third-party processor will not be valid, because consent must be unambiguously freely given[7] and be able to be refused without prejudice.[8]

It is important to remember that the data-protection rules are not applied in isolation from the legislation on educational settings or law on equality, employment, privacy of communications and other relevant and domestic law.

The guidelines should be applied together with the existing principles of data protection highlighted in section 4, including the principle of data minimisation.

---

7. In accordance with Article 5(2) of Convention 108+ and in this context, it should also be taken into account that recital 43 of the GDPR states that "in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation" and that children in an educational setting constitute a typical example of a situation where there is an imbalance between the data subject and the controller and where another legal basis should rather be applied.
8. As set out in paragraph 42 of the Explanatory Report to Convention 108+, "No undue influence or pressure (which can be of an economic or other nature) whether direct or indirect, may be exercised on the data subject and consent should not be regarded as freely given where the data subject has no genuine or free choice or is unable to refuse or withdraw consent without prejudice".

Adults should ensure that protections offered to children are not only appropriate for the duration of their childhood but also consider children's future interests. We have a duty to promote the ability of children to reach maturity unimpeded and to be able to develop fully and freely, to meet their full potential and to foster human flourishing.

# 2. Scope and purpose

2.1. These guidelines seek to help explain the data-protection principles of Convention 108+, to tackle the challenges in the protection of personal data brought about by new technologies and practices, while maintaining technologically neutral provisions.

2.2. The guidelines aim to ensure that the full range of the rights of the child are met as pertains to data protection as a result of interactions with an educational setting, among which are the rights to information, to representation, to participation and to privacy. They should be fully respected and should give due consideration to the child's level of maturity and understanding.

2.3. Nothing in the guidelines shall be interpreted as precluding or limiting the provisions of the European Convention on Human Rights and of Convention 108.[9] These guidelines also take into account the new safeguards of Convention 108+.

2.4. The guidelines remain general in nature. Supervisory authorities may wish to address practical suggestions in relation to educational settings, including checklists for those that want to integrate digital technologies into their processes as part of domestic codes of practice and practical guidance specific to states parties' law. Codes of practice could be also submitted (for approval) to supervisory authorities (among the competent authorities). States should develop evidence-based standards and guidance for schools and other bodies responsible for procuring and using educational technologies and materials to ensure these deliver proven educational benefits and uphold the full range of children's rights.

9. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

# 3. Definitions for the purposes of the guidelines

a. "Child" means every human being below the age of 18 unless the age of majority is attained earlier under the national law.

b. "Data analytics" refers to personal data used in the computational technologies that analyse large amounts of data to uncover hidden patterns, trends and correlations and refers to the whole data management life cycle of collecting, organising and analysing data to discover patterns, to infer situations or states, to predict and to understand behaviours.

c. "Digital environment" is understood as encompassing information and communication technologies, including the internet, mobile and associated technologies and devices, as well as digital networks, databases, applications and services.

d. "Direct care and education" means a learning, administrative or social-care activity concerned with the direct delivery of teaching and its administration, or the immediate care of an identified individual, generally falling within the statutory public tasks of education and the data processing, for which the child and legal guardians would reasonably expect as part of being in school. Direct care is contrasted with "secondary reuses" of data, which are all other indirect uses of personal data collected or inferred about an individual in the context of their time spent "*in loco parentis*" with an educational setting; non-exhaustive examples include learning analytics, risk prediction, public interest research, for processing in the press or on social media, and marketing purposes.

e. "Educational setting" means an environment for the delivery of education to a child, subject to the jurisdiction of states parties in the private and public sectors, but not by an individual in the course of purely household activities.

f. "e-Learning" may broadly include learning with the support of information and communication technologies, especially for delivery or accessing of content, distance learning or web-based learning (including tools used in online and offline modes). e-Learning can take place without any live connection to a network or internet connectivity but will often requires such access as part of the service.

g. "Legal guardians" refers to the persons who are considered to hold parental responsibilities for the child according to national law and have the collection of duties, rights and powers that aim to promote and safeguard the rights and welfare of the child in accordance with the child's evolving capacities.

h. "Learning analytics" can be described as the measurement, collection, analysis and reporting of data about learners and their contexts, for the purposes of understanding and optimising learning and the environments in which it occurs.[10]

i. "Processing" means any operation or set of operations performed on personal data, such as but not only the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure or destruction of, or the carrying out of logical and/or arithmetical operations on such data.

j. "Profile" refers to a set of characteristics attributed to an individual, characterising a category of individuals or intended to be applied to an individual.

k. "Profiling" refers to any form of automated processing of personal data including use of machine learning systems consisting of the use of personal or non-personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

---

10. Learning and Academic Analytics, Siemens G., 5 August 2011: www.researchgate.net/publication/254462827_Learning_analytics_and_educational_data_mining_Towards_communication_and_collaboration.

l. "Special category of data" has the same meaning as that in Article 6 of Convention 108+.

m. "Supervisory authorities" means authorities designated as being responsible for ensuring compliance with the provisions of Chapter IV of Convention 108+.

# 4. Principles of data processing

Convention 108+ lays down the following principles, obligations and rights which apply to any processing of personal data and are therefore essential to apply in an educational setting.

4.1. Legitimacy of the processing, and the principles of lawfulness, fairness, necessity, proportionality, purpose limitation, accuracy, limited time retention in identifiable form, transparency and data minimisation must be ensured and it must be guaranteed that personal data are adequate, relevant and not excessive in relation to the purposes for which they are processed in accordance with Article 5 of Convention 108+.

4.2. A precautionary approach and strengthened protection towards sensitive, special categories of data, including genetic and biometric data, and those data relating to ethnic origin, sexual orientation or offences, must be guaranteed recognising children's additional vulnerability (Article 6 of Convention 108+).

4.3. Meaningful transparency of data processing must be ensured, recognising the importance of accessibility through the use of clear language, in child-friendly terms and formats when appropriate, in communication, offline or online, and on any device, in accordance with Article 8 of Convention 108+.

4.4. The accountability of data controllers and data processors must be clearly set out in any contractual arrangements, defined by the nature of the processing, in accordance with Article 10, paragraph 1, of Convention 108+.

4.5. The principles of privacy and data protection by design and suitable organisational and technical measures should be applied in practice (Article 10, paragraph 2, of Convention 108+).

4.6. An assessment of the likely impact of the intended processing on the rights and freedoms of the data subject prior to the commencement of any data processing and across its life cycle should be carried out. Particular attention needs to be paid at an early stage to how communication about data processing will be maintained between the data controller and the child or their legal guardian, after the child has left the educational setting.

4.7. Security measures[11] are necessary to prevent and protect against risks, such as accidental or unauthorised access to, destruction, loss, misuse, modification, ransom demands or disclosure of personal data.

4.8. Specific to the educational context, data controllers must recognise the rights of legal guardians to act on behalf of and in their child's best interests in accordance with domestic and international law, and in accordance with Article 9 of Convention 108+. The best efforts should be made to involve a child in decisions about them and provide suitable information to families, where appropriate.

11. Suggested reference on security of personal data during remote learning – UODO's guide for schools https://uodo.gov.pl/en/553/1118.

# 5. Fundamental principles of children's rights in an educational setting

The guidelines build on the existing principles enshrined in Convention 108+, the Council of Europe Strategy for the Rights of the Child (2016-2021)[12] and the case law of the European Court of Human Rights. Every child is entitled to enjoy the full range of human rights safeguarded by the European Convention on Human Rights, the United Nations Convention on the Rights of the Child (UNCRC) and other international human rights instruments. These guidelines encourage states parties to Convention 108 to recognise these rights in the context of children's data protection in education. With a view to guaranteeing the best interests of the child in all measures affecting them, states parties may consider introducing and enhancing the quality and effect of child impact assessments in accordance with the Council of Europe Strategy for the Rights of the Child (2016-2021).

## 5.1. Best interests of the child

5.1.1. The best interests of the child shall be a primary consideration in all actions concerning the child in the digital environment.

5.1.2. In assessing the best interests of a child, states should make every effort to balance and reconcile a child's right to protection with other rights, in particular the right to freedom of expression and information, the right to participation and the right to be heard.

12. The Council of Europe Strategy for the Rights of the Child (2016-2021):https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168066cff8.

5.1.3. Specific considerations may need to be given to the definition of "best interests" to more vulnerable children in education, such as those without parents, migrant children, refugee and asylum-seeking children, unaccompanied children, children with disabilities, homeless children, Roma children and children in residential, medical or young offender institutions.

## 5.2. Evolving capacities of a child

5.2.1. The capacities of a child evolve from birth to the age of 18. Individual children reach different levels of maturity at different ages.

5.2.2. As set out in the Guidelines to respect, protect and fulfil the rights of the child in the digital environment,[13] all stakeholders should recognise the evolving capacities of children, including those of children with disabilities or in vulnerable situations, and ensure that policies and practices are adopted to respond to their respective needs in relation to the digital environment.

## 5.3. Right to be heard

5.3.1. Children have the right to express themselves freely in all matters affecting them, and their views should be given due weight in accordance with their age and maturity. States should make sure that children are aware of their rights in the digital environment in a child-friendly, transparent, comprehensible and accessible way. Everyone in the education system should ensure children are able to access mechanisms for enforcing their rights.

5.3.2. Staff in educational settings should establish a default position of good practice to involve legal guardians and children, according to their capacity, in consultation about decisions to adopt new technology that result in the processing of children's personal data, to ensure a fair balance of all interests concerned, aligned with Article 5, paragraph 1, of Convention 108+. States should also ensure that consultative processes are inclusive of children who lack access to technology[14] at home.

---

13. Council of Europe Guidelines to respect, protect and fulfil the rights of the child in the digital environment, Recommendation CM/Rec(2018)7: https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a.
14. United Nations Committee on the Rights of the Child, General Comment on children's rights in relation to the digital environment, August 2020: https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2f5F0vEG%2bcAAx34gC78FwvnmZXGFUl9nJBDpKR1dfKekJxW2w9nNryRsgArkTJgKelqeZwK9WXzMkZRZd37nLN1bFc2t.

5.3.3. According to Article 5, paragraph 4.*a*, of Convention 108+, legal guardians and children should both be fairly informed of data processing, unless sharing such information poses a risk to the best interests of the child, with due regard to Article 11.*b* of the Convention, or unless a competent child makes an objection to the involvement of one or more legal guardian.

5.3.4. In accordance with states parties' law, including taking into account any age limits set out in law for consent to data processing by information society services (ISS) where the definition of an ISS is applied in an educational setting, and to support the child as data subject, legal guardians should be permitted to exercise rights under Article 9, paragraph 1.*b*, of Convention 108+, on behalf of the child in education, where the child does not object, taking into account their level of capacity and the best interests of the child.

5.3.5. Data processing on the basis of consent may be invalid where a power imbalance exists, notably between a public authority and an individual, which impairs the freely given nature of the consent. This imbalance is even more significant where the data subject is a child. Another basis is therefore more likely to be valid for routine processing activities and such processing should be based in law.

5.3.6. Children should be enabled by the provision of child-friendly, transparent, comprehensible and accessible information on the data processing to both give and withhold consent where they have the capacity to understand the implications, and processing is in their own best interests, and in line with any age-based laws in domestic and international legislation.

5.3.7. Children should have the right to access appropriate, comprehensible, independent and effective complaints mechanisms and exercise their rights.

## 5.4. Right to non-discrimination

The rights of the child apply to all children without discrimination on any grounds. Whereas efforts should be undertaken to respect, protect and fulfil the rights of each and every child in an education setting, targeted measures may be needed to address specific needs, recognising that the digital environment has the potential to increase children's vulnerability and to empower, protect and support them.

# 6. Recommendations for legislators and policy makers

The use of digital technologies for educational purposes leads to the processing of personal data of children by a variety of actors (including national governments, public and private educational establishments, commercial enterprises such as providers of products or services, software developers and individuals such as teachers, legal guardians and peers). The data that are processed are not only provided by children, parents or educators but are also created as a by-product of user engagement or can be data that are inferred (for instance on the basis of profiling). Highly sensitive data, such as biometric data, are increasingly collected by educational institutions. Such data collection may have lifelong implications for children. Since situations arise when different authorities are under a legal obligation to co-operate, a strict necessity and proportionality test should be applied before the collection of all personal data to ensure data minimisation and that any use will meet a child's reasonable expectations and meet the principles of purpose limitation and comply with restrictions on storage and retention. It is essential to acknowledge that it is not only the child's right to data protection that is affected when it comes to education and digital technologies but also that the right to privacy and data protection are enabling rights for the protection of further rights and of the child. The right to non-discrimination, the right to development, the right to freedom of expression, the right to play and the right to protection from economic exploitation might also be at stake. Legislators and policy makers should ensure that the full range of rights are ensured by other instruments, protocols and guidelines when considering the implications of children's data processing in the context of education.

## 6.1. Review legislation, policies and practice

Legislators and policy makers should

6.1.1. Ensure alignment with the present guidelines and promote their implementation in all data processing in, across and after leaving the educational setting for the whole of the data life cycle.

6.1.2. Set high expectations for privacy-by-design configurations in standards for the technical requirements of procured services.

6.1.3. Maintain or establish a framework, including independent mechanisms as appropriate, to promote and monitor the implementation of these guidelines, in accordance with their educational, supervisory and administrative systems.

## 6.2. Offer effective support for children's right to be heard

Legislators and policy makers should

6.2.1. Provide supervisory authorities with sufficient resources to ensure that data-protection laws are adequately applied in the educational setting and related technologies used consistently.

6.2.2. Representation of child data subjects to supervisory authorities (Article 18) by third parties should be accessible and strengthened. States parties may provide under Article 13 for extended protection in their legislation. It should be made possible that any body, organisation or association independent of a data subject's mandate has the right to lodge a complaint with the competent supervisory authority, in that state party, where permitted by the law, if it considers that the rights of a data subject have been infringed as a result of processing.

6.2.3. Establish procedures for children to express themselves and to make their views heard with regard to exercising their right to privacy in educational settings and to ensure their view is taken into consideration.

6.2.4. Make it easy for a child to access remedies for violations of the provisions of the Convention under Article 12 and, in the spirit of the Council of Europe Guidelines on child-friendly justice,[15] remove any obstacles for children to

15. Guidelines on child-friendly justice adopted by the Committee of Ministers of the Council of Europe on 17 November 2010. See also Parliamentary Assembly Resolution 2010 (2014) "Child-friendly juvenile justice: from rhetoric to reality", and the orientations on promoting and supporting the implementing of the Guidelines on child-friendly justice by the European Committee on Legal Co-operation (CDCJ (2014)15).

obtain access to court, providing the grounds for necessary co-operation, and with mutual assistance between supervisory authorities (Articles 15, 16 and 17, paragraph 3, of Convention 108+) in matters concerning data protection in an educational setting.

6.2.5. Recognising that specific attention shall be given to the data protection rights of children and other vulnerable individuals, educational institutions shall ensure that staff are trained to ensure adequate capability to understand their role in due diligence, and to be able to incorporate the right of the child to be heard.

## 6.3. Recognise and integrate the rights of the child

Legislators and policy makers should

6.3.1. Respect and fulfil the obligations and commitments within existing Council of Europe and United Nations standards on the rights of the child.[16] These guidelines apply to all children, with a view to realising this right to education without discrimination, and on the basis of equal opportunity.

6.3.2. Respect, protect and fulfil the rights of the child in the digital environment in an educational setting, in accordance with the Guidelines on children in the digital environment.[17]

6.3.3. Respect the UN General Comment No. 16 (2013) on state obligations regarding the impact of the business sector on children's rights.[18] States must take steps to ensure that public procurement contracts are awarded to bidders that are committed to respecting children's rights, and states should not invest public finances and other resources in business activities that violate children's rights. States should take appropriate measures to prevent, monitor

16. The UNCRC Article 29.1: "States Parties agree that the education of the child shall be directed to: (a) The development of the child's personality, talents and mental and physical abilities to their fullest potential; (b) The development of respect for human rights and fundamental freedoms, and for the principles enshrined in the Charter of the United Nations". www.ohchr.org/en/professionalinterest/pages/crc.aspx and Principle 7 Declaration of the Rights of the Child (1959) (Proclaimed by the UN General Assembly, resolution 1386 (XIV), A/RES/14/1386, 20 November 1959).
17. Council of Europe Guidelines to respect, protect and fulfil the rights of the child in the digital environment, Recommendation CM/Rec(2018)7: https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a.
18. Committee on the Rights of the Child General Comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights: www.unicef.org/csr/css/CRC_General_Comment_ENGLISH_26112013.pdf. For some children the use of adaptive technology can be an unwelcome signifier of their disability.

and investigate violations by businesses in the educational setting and digital environment.

6.3.4. Recognise the obligations in Article 24 in the Convention on the Rights of Persons with Disabilities to education and with regard to inclusion and involvement in the decision making about adoption of technology, ensure universal accessibility by design and promote equitable provision.

# 7. Recommendations for data controllers

There are many actors in the data processing chain who may be data controllers, not only educational institutions and government bodies but also providers of platforms, devices, programmes and applications. The latter commercial actors may also be data controllers in their own right, where they alone or jointly with others determine the nature of the processing as defined in Article 2 of Convention 108+, and careful attention is needed to understand that the nature of the processing determines each role and not solely what is set out in contract terms. The obligations upon data controllers may not always fall solely on the educational establishment as a result. To meet all the relevant data-protection principles, including data accuracy, necessity and security, educational institutions need to encourage a comprehensive and compliant data governance culture in which risk assessment proactively considers rights and freedoms as part of any processing or procurement process and data quality is proactively monitored and effectively managed through records management, supported by training and policies.

## 7.1. Legitimacy and lawful basis

7.1.1. According to paragraph 1 of Article 10 of Convention 108+, the obligation rests with the controller to ensure adequate data protection and to be able to demonstrate that data processing is in compliance with the applicable laws.

7.1.2. All parties involved in data processing in educational settings should clarify the responsibilities and accountability between roles to establish legal authority and their duties as regards data processing, and when contracting with providers and third-party data processors.

7.1.3. A child's special category data, as defined in Article 6 of Convention 108+, requires enhanced protection when being processed, starting with the appropriate legal basis for the processing. Where there is no other lawful basis for processing, informed and freely given consent should be obtained from a legal guardian for the processing of health and other special categories of data, and recorded as an appropriate safeguard under Article 6, paragraph 1, of Convention 108+), when processing is in the best interests of the child. Such special category data may be shared for purposes that go beyond their direct care and education, only with freely given, specific, informed and explicit consent of the data subject or their legal guardian.

7.1.4. Consent for any data processing, including but not limited to a child's special category of data, can never be assumed, on behalf of legal guardians or children, to legitimise data processing by third-party providers.

7.1.5. Data controllers should recognise that children and legal guardians cannot give valid consent to the use of third-party data processors where it cannot be freely refused and without prejudice.

7.1.6. The legal guardians' powers to exercise rights on behalf of a child as a data subject expire when the competent child reaches the age of maturity as laid down in law. The data subject (the child) should be informed of any ongoing data processing about them to which the legal guardian gave consent, so as to be able to exercise the rights of the data subject as an adult.

7.1.7. Children should not be expected to enter into a contract with third parties, for example with an e-learning provider or application mandated by the educational institution. The educational institutions should process children's data on the basis of a written contract between them and the third party. Personal data processing by such services should be carried out on a legitimate basis laid down by law.

7.1.8. Contracts between third parties and education providers should prevent any changes of terms and conditions that affect the fundamental rights and freedoms of the data subject. Any changes to contracts between third parties and education providers would by default require a revision of the contract and notification to the data subject (or their legal guardians as appropriate) explaining the proposed changes in a clear and straightforward way.

7.1.9. To meet the obligation of the right of a child to education, institutions should offer a suitable level of alternative provision of education without prejudice to the child, should families or the child exercise the right to object to data processing in digital tools, as a remedy in accordance with Article 9, paragraph 1.*f*, of Convention 108+.

7.1.10. In line with Article 9, paragraph 1.*d*, of Convention 108+, advertising should not be considered legitimate grounds or a compatible purpose under Article 5, paragraph 4.*b*, that overrides a child's best interests, or their fundamental rights and freedoms.

7.1.11. Data analytics and product development using personal data should not be considered legitimate compatible use for further processing that override a child's best interests or rights and fundamental freedoms, or reasonable expectations of the data subjects in accordance with paragraph 49 of the Explanatory Report to Convention 108+.

7.1.12. Controllers and processors shall not give away children's personal data collected in the course of their education, for others to monetise, or reprocess them for the purposes of selling anonymised or de-identified data, for example to data brokers.

7.1.13. The further processing of personal data, referred to in Article 5, paragraph 4.*b*, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, is compatible where the purposes are as defined in paragraph 50 of the Explanatory Report to Convention 108+.

7.1.14. Consistent with states parties' domestic law, codes of practice should set out guidance for situations where staff or children access educational software systems, databases or other third-party products through personal electronic devices or from home, and therefore mix personal data, including metadata, from their private and family life with their professional or educational record.

## 7.2. Fairness

7.2.1. In accordance with Article 5, paragraph 4.*a* of Convention 108+, data shall be processed fairly and in a transparent manner. Article 8, paragraphs 1.*a* to *e*, of Convention 108+ sets out what is expected to meet the requirement that data processing is transparent and complete. In accordance with paragraph 68 of the Explanatory Report to Convention 108+, the format can be any way that provides information fairly and effectively to a data subject. That means, for example, according to the child's evolving capacity and in child-friendly, comprehensible language and accessible alternative formats to text-only where appropriate. It should be interpreted in the educational context as necessary to be understood by a competent child, or by their legal guardians for younger children, or as appropriate for the evolving capacities of the child.

7.2.2. Proactive provision of accessible information about the full range of data subject rights, available to the child and his or her legal guardian prior to the start of a data collection process, is necessary to meet transparency obligations. As a rule, both the child and legal guardians should receive the information directly. Provision of the information to the legal guardian should not be an alternative to communicating the information to the child, appropriate to their evolving capacity.

7.2.3. Educational institutions should carry out and publish a register of their data processing activities, a list of partners, such as vendors and subcontractors, data protection impact assessments, privacy notices and any amendments to terms and conditions over time.

7.2.4. Educational institutions should report to supervisory authorities as prescribed by Convention 108+ and to the data subjects themselves in the event of breaches in accordance with Article 7, paragraph 2, of the Convention and share audit reports to demonstrate their accountability and transparency of data processing with third parties.

7.2.5. Statements about personal data processed should be available on request, as part of subject access rights. It may be recognised as good practice to offer such information through self-service tools, free to the child as the data subject.

7.2.6. Before transborder flows of personal data and subject to appropriate levels of protection according to Article 14, paragraphs 3 and 4 of Convention 108+, the data subject and their legal guardians should be informed.

## 7.3. Risk assessment

7.3.1. Controllers must assess the likely impact of intended data processing on the rights and fundamental freedoms of the child, prior to the commencement of data processing, in accordance with Article 10, paragraph 2, of Convention 108+, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms, with regard to Article 10, paragraph 3, of Convention 108+ and all its other principles.

7.3.2. The procurement of tools and services that process children's data shall ensure respect for children as data subjects and their legal guardians' rights and their reasonable expectations, as part of the decision making when introducing any product, whether it is bought or is freeware.

7.3.3. Where freedom of information laws apply to public bodies, codes of practice could include a suggestion as best practice that data-protection impact assessments may be made accessible as part of routine publication schemes, to facilitate broad transparency and accountability.

7.3.4. As best practice, and in accordance with domestic and international law, children's views should be part of any impact assessment of children's rights carried out in order to include their perspective with regard to their data processing.

## 7.4. Retention

7.4.1. At the time when a child leaves education, only the minimum necessary amount of identifying data should be retained, and in the child's best interests, in order to demonstrate attainment, to safeguard their future rights of access and to meet statutory obligations.

7.4.2. Personal data that leave an educational institution should not be preserved in a form that permits identification for any longer than necessary, in accordance with Article 5, paragraph 4.*e*.

7.4.3. Educational institutions should not retain personal data in a form which permits identification for longer than necessary, and with due regard to the provisions of Article 5, paragraph 4; Article 7, paragraph 2; Article 8, paragraph 1; and Article 9 of Convention 108+. Exceptions that respect the essence of the fundamental rights and freedoms of the child and constitute a proportionate measure, necessary in a democratic society for the purposes of Article 11 of Convention 108+, may apply.

7.4.4. Upon leaving each stage of compulsory education or when they change institution (across all ages; in nursery, primary, secondary, further or tertiary education), it should be best practice for children to receive a full copy of their record including information about personal data retention and destruction, that is, to be informed which personal data continue to be retained and processed, by whom and for what purposes, after the child has left the institution, and in any case the data controllers must maintain mechanisms that enable them to fulfil any ongoing obligations to the data subject.

7.4.5. Because it is so difficult to de-identify data well, best practice should be to prohibit re-identification and require that third parties do not attempt any re-identification or allow others to do so after receipt of de-identified data, and recognise, where it applies according to domestic law in some state parties, that re-identification may be a criminal offence.

## 7.5. Securing personal data in an educational setting

Educational institutions can be involved in processing children's data on a large scale over long periods of time. Applying appropriate security measures to these data, and its processing environments both at rest and in transit, is vital to ensure children's data are protected to the highest standards. As Convention 108+ sets out, security measures should take into account the current state-of-the-art of data security methods and techniques in the field of data processing. Their cost should be commensurate with the seriousness and probability of the potential risks. Data security encompasses further obligations and the controls listed below are particularly relevant for processing within educational settings.

7.5.1. The protective measures applied to personal data should be based on a risk assessment following industry standards and best practice and using established technical guidance (such as the ISO 27000 series and others as appropriate).

7.5.2. Measures should be particular to the circumstances of the processing and the risks posed to the children involved, and be aimed at ensuring the confidentiality, integrity, availability and authenticity of children's data in whatever context they are processed, as well as the resilience of processing systems and services.

7.5.3. Risk assessment should therefore seek to achieve outcomes that embed high standards of security throughout the processing, taking into account its nature, scope, context and purposes as well as the risks it poses. Such an assessment must be informed by considerations of necessity and proportionality, and the fundamental data-protection principles:

- ▶ protection against a range of risks, including physical accessibility;
- ▶ networked access to devices and data;
- ▶ the backup and archiving of data.

7.5.4. Physical accessibility (for example, to devices and data in the educational institutions) includes data collected or stored in at least the following contexts:

- ▶ classroom/e-learning (including distance learning outside school premises);
- ▶ school administration;
- ▶ premises (physical access, CCTV, including that on school vehicles, biometric readers).

7.5.5. Consideration must be given to how child users should authenticate themselves to systems, including when this is required within the context of the processing. Risk assessments should consider the authentication methods any deployment requires, giving due consideration to alternative approaches where these are available and preserve user privacy, such as fully identifiable ID and password systems or tokens and attribute-level authorisation. Authentication should be robust and capable of ensuring that data are protected. The principles of purpose limitation and data minimisation should also form part of the assessment of any authentication system.

7.5.4. For networked access to data, authentication is almost certain to be required, and is desirable, to prevent unauthorised access. The same questions arise as do for on-site access: what is the most appropriate authentication technology, and is access granted on the basis of individual identity (first name, last name) or an attribute ("pupil at this school")?

7.5.5. Risk assessment prior to processing must also assess whether data are protected against unauthorised access, modification and removal/destruction. Where data are processed off site (for example, by third-party service providers), education providers must remain aware of their ongoing responsibilities as data controllers. Due diligence must be carried out to establish the third party's ability to protect personal data appropriately, including confidentiality, integrity and availability.

7.5.6. Similar questions should be asked relating to digital data that are stored for backup and/or archival purposes, especially if these services are provided by third parties – either explicitly (such as for a contracted archival service) or implicitly, as part of the data availability protections offered by an e-learning, administrative service.

7.5.7. States parties should not prohibit in law or practice the usage of encryption technologies for children.[19] Where encryption is not integrated into an application or service, it may be desirable to encrypt data "manually" as a stand-alone protective measure.

7.5.8. Numerous levels of protection can be applied (and even combined). Encrypted data should be managed in a similar way to backup/archive data. That is, the process of getting the data back again (from their encrypted state, or from their backup location or archive) should be regularly tested. Consideration should be given to fallback procedures in case the person primarily responsible cannot perform this task.

19. Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment.

7.5.9. Any measures put in place should be regularly tested, as set out in Article 7 of Convention 108+ and take into account the changing data-security methods, techniques and risks and be kept under regular review and updated where necessary.

## 7.6. Automated decisions and profiling

7.6.1. Every individual has the right not to be subject to a decision significantly affecting him/her based solely on an automated processing of data without having his or her views taken into consideration in accordance with Article 9, paragraphs 1.*a* and 1.*c*, of Convention 108+. Knowledge of the reasoning underlying the data processing where the results are applied to the data subject, should be made readily available.

7.6.2. Profiling of children should be prohibited by law. In exceptional circumstances, states may lift this restriction when it is in the best interests of the child or if there is an overriding public interest, on the condition that appropriate safeguards are provided for by law (in accordance with paragraph 37 of the Guidelines to respect, protect and fulfil the rights of the child in the digital environment).

7.6.3. Children's attainment and achievement should not be routinely profiled in order to assess systems, for example, for measuring school or teacher performance management on the basis that this is not justified as an overriding public interest.

7.6.4. The Guidelines on artificial intelligence and data protection[20] should be followed in educational settings with regard to the automatic processing of personal data to ensure that artificial intelligence applications do not undermine the human dignity, the human rights and fundamental freedoms of every child, whether as an individual or as part of a community in particular with regard to the right to non-discrimination.

7.6.5. Recognition of the rights of the child, as the data subject, and their legal guardians, is necessary in an algorithmic decision-making context, associated with processing personal data using artificial intelligence, and in informed processing (see the Guidelines on artificial intelligence and data protection).[21]

20. Guidelines on artificial intelligence and data protection, document T-PD(2019)01, available at https://rm.coe.int/2018-lignes-directrices-sur-l-intelligence-artificielle-et-la-protecti/168098e1b7.
21. Ibid.

7.6.6. Data controllers have the responsibility to carry out data-protection and privacy impact assessments. These should have regard for the specific impact on children's rights[22] and should demonstrate that the outcomes of algorithmic applications are in the best interests of the child and ensure that a child's development is not unduly influenced in opaque ways.

7.6.7. Personalisation of content may (but does not always) constitute an intrinsic and expected element of certain online services, and therefore may be regarded as necessary for the performance of the contract in some cases between the service supplier and the educational institution, but not in respect of the child since they cannot enter into a contract[23] even at the insistence of the institution.

7.6.8. Predictions about groups or persons with shared characteristics based on analysis of large sets of personal data shall still be considered as processing personal data, even where there is no intention for it to result in an intervention with an individual.

7.6.9. The distribution and use of software or use of services designed to observe and monitor user activity on a terminal or communication network in order to build a profile of behaviour should not be permitted, unless expressly provided for by domestic law and accompanied by appropriate safeguards, as set out in Principle 3.8 of Council of Europe Recommendation CM/Rec(2010)13 and explanatory memorandum[24] on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

## 7.7. Biometric data

7.7.1. Biometric data should not be routinely processed in educational settings. The use of biometrics in educational settings in exceptional circumstances, such as for identity verification including remote supervision of examinations, shall only be allowed where no less intrusive method may achieve the same aim, in accordance with the principle of strict necessity, after carrying out a data-protection impact assessment and with appropriate safeguards enshrined in law, in accordance with Article 6, paragraph 1, of Convention 108+. This

22. Committee on the Rights of the Child General Comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights paras 77-81: www.unicef.org/csr/css/CRC_General_Comment_ENGLISH_26112013.pdf.
23. See EDPB, Guidelines 2/2019.
24. Council of Europe Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling and explanatory memorandum (2011) https://rm.coe.int/16807096c3.

should include due regard for the risks that the processing of sensitive data may present for the rights and fundamental freedoms of the child, including lifelong discrimination. Alternative methods should be offered without prejudice.

7.7.2. Biometric applications aiming at providing support to children and educational staff with accessibility needs, for example on-screen eye tracking, for their direct benefit and without discrimination,[25] should be provided for with appropriate safeguards enshrined in law.

7.7.3. Recognising that within Article 6 of Convention 108+, biometric data are defined as being uniquely for identifying a person, authorities should also be alert to the sensitivity of processing bodily and behavioural data from a child that may not be for verification of identity. The purposes of such data processing may be instead to influence the physical or mental experience of the child, such as in immersive virtual reality. Processing characteristics about voice, eye movement and gait; social, emotional and mental health, and mood; and reactions to neurostimulation, for the purposes of influencing or monitoring a child's behaviour, should be done on the basis of a precautionary principle and treated as biometric data are under Convention 108+, even when they are not for the purposes of uniquely identifying the person.

7.7.4. Educational institutions should pay particular attention to where their use of a service constitutes a contractual agreement, for example in the use of videoconferencing software in order to be able to implement distance-learning programmes, and in which staff may agree to the terms and conditions of a service that include the processing and recording of content including children's images and voice data. Staff should ensure that where data processing is carried out on the basis of consent, that consent cannot be assumed by the educational institution and granted on behalf of the child, but must be informed and unambiguously and freely given by the data subject, the child, in accordance with their evolving capacities, or their legal guardian, and in accordance with all other data protection principles, including purpose limitation.

25. Two clicks forward, and one click back: Report on children with disabilities in the digital environment (2019), Council of Europe (page 5) "For these children, the technology is a somewhat unwelcome signifier of their disability." https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f.

# 8. Recommendations for the industry

Supervisory authorities that develop these guidelines into codes of practice should do so on the basis of wide co-operation with developers and the industry, with education practitioners and academia, with organisations representing teachers and families, and with civil society and children themselves. Standards may include minimum criteria or clear guidelines for procurement in relation to products or services concerning children's data processing, including products or services offered for free or at a low cost, and in any product and research trials.

## 8.1. Standards

8.1.1. Since children merit special protection, the expected standards for the processing of children's data in the education sector should set a high bar by design, to meet appropriate standards of quality and the rule of law, and data protection by design and by default.

8.1.2. Standards may be set out in codes of practice and certification that should be drafted on the basis of wide co-operation with developers and the industry, with education practitioners and academia, with organisations representing teachers, families and children, with civil society and with children themselves.

8.1.3. Provisions of lawful data processing contracts, agreed at the time of the procurement, should also continue to apply after the purchase, merger or other acquisition by another entity. There must be a sufficiently fair communication period of any change of terms and the right to alter or object to new conditions, end the contract and withdraw student data on request.

## 8.2. Transparency

8.2.1. Developers must ensure that their own understanding of all the functionality of products they design can be sufficiently explained to meet regulatory and lawful requirements, and avoid creating a high investigative burden by design, inappropriate for staff in education settings and children.

8.2.2. Privacy information and other published terms and conditions, policies and community standards must be concise and written in clear language appropriate for children. Child-friendly communication methods need not dilute the explanations that are necessary for fair processing but should not be excessive and should be separate from legal and contractual terms for legal guardians and educators. Layered privacy notices could help to combine the need for simultaneously complete and efficient information.

## 8.3. Design features with data protection and privacy implications

8.3.1. Expectations of respect for the principles of data protection by design and default should prevent design that includes features that may encourage children to provide unnecessary personal data or to lower their privacy settings.

8.3.2. Processing personal data for the purposes of service improvement and security must be strictly necessary and within the confines of the delivery of the core service as well as the reasonable expectations and delivery of the contracted service to users.

8.3.3. Data analytics[26] based on personal data and user tracking should not be considered a form of service improvement or security enhancement and not be necessary for the fulfilment of a contract.

8.3.4. Product enhancements, for example those intended to add new features to an application or improve its performance, should require new acceptance or consent as well as an opt-in before installation. Where another lawful basis is relied upon other than a contract, the data subject must be informed ahead of the upgrades and in accordance with the lawful basis.

8.3.5. Specific attention should be given to Article 14 of Convention 108+ to make sure transborder flows of personal data for the purposes of education meet the conditions of the article, to limit transborder flows of personal data

26. Guidelines on the protection of individuals on the processing of person data in a world of Big Data (2017), T-PD(2017)01.

for the purposes of education and to ensure that transborder flows take place within a recognised data-protection framework.

8.3.6. Geolocation tracking in order to identify the location of use, the user, to target in-app functionality or for profiling purposes should be deployed only when necessary and according to an appropriate legal basis. Services should provide an indicator when the location tracking is active and allow easy disabling without loss of essential functionalities. Such profiles and history should be easy to delete at the close of a session.

8.3.7. Children's data collected by means of educational software tools should not be processed to serve or target behavioural advertisements, for real-time bidding advertising technology or for in-app advertising, or to provide marketing messages about product upgrades or additional vendor-driven products to children or families.

The digital environment shapes children's lives in many ways, creating opportunities and risks to their well-being and enjoyment of Human Rights.

This applies in the everyday life but also increasingly in education settings where tools designed for teaching, supervision, assessment of children are deployed without the various actors always being aware of the challenges to children's private life and personal data protection.

The introduction of digital tools to the classroom in effect opens up the school gates to a wide range and high volume of stakeholders who interact with children's everyday activities. The majority of the devices and applications, software and learning platforms, adopted in educational settings are developed by private, commercial actors.

The Guidelines on Children's Data Protection in an Educational Setting aim at supporting organisations and individuals in the context of education to respect, protect and fulfil the data protection rights of the child in the digital environment, within the scope of Article 3 of the modernised Convention 108 (more commonly referred to as "Convention 108+"), and in accordance with the CoE instruments including the Guidelines on Children in the Digital Environment Recommendation CM/Rec(2018)7.

**www.coe.int/dataprotection**

PREMS 001721

ENG

**www.coe.int**

The Council of Europe is the continent's leading human rights organisation. It comprises 47 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE