esha

2025

#20

HEADSTART

THE IMPACT OF GDPR AND CHILDREN'S DATA RIGHTS

ON THE DAILY PRACTICES OF SCHOOL HEADS

ESZTER SALAMON

#Practical question for which this card offers SUGGESTIONS:

What data handling procedures are necessary to create a legally compliant school environment?

The General Data Protection Regulation (GDPR) and the UN Convention on the Rights of the Child (UNCRC) have a significant impact on how schools handle student data. School heads, as key administrators, must navigate these regulations to ensure compliance, protect student privacy, and uphold children's rights. This Headstart examines how these regulations influence daily practices, focusing on data collection, consent procedures, and the sharing of photos and videos.

Data Collection: What Can Be Collected and How?

GDPR mandates that schools must have a legal basis for collecting student data. The types of data that schools can collect generally fall into the following categories:

1. **Personal Identification Data:** Includes names, dates of birth, addresses, and student ID numbers.
2. **Academic Records:** Attendance, grades, standardized test scores, and teacher assessments.
3. **Health Information:** Allergies, medical conditions, emergency contact details (special category data under GDPR, requiring extra protections).
4. **Behavioural Data:** Disciplinary records, participation in extracurricular activities, and student conduct reports.
5. **Parental and Guardian Information:** Contact details for communication regarding the student.
6. **Digital Data:** Email accounts, learning platform usage data, and biometric data (if applicable).

Collection Methods Schools must ensure that data collection methods comply with the following key GDPR principles:

- **Minimization:** Only collect data necessary for educational purposes.
- **Transparency:** Inform students and guardians about what data is collected and why.
- **Security:** Implement technical and organizational measures to prevent unauthorized access or data breaches.
- **Retention Policy:** Clearly define how long the data will be stored and when it will be deleted.

Consent Procedures: Ensuring Legal Compliance

Consent plays a vital role in data processing in schools. Schools often rely on **legitimate interest** or **public interest** as a legal basis instead of consent for routine data processing. It is important to clearly define what really is legitimate or public interest, and to not overreach.

When consent is required, schools need to consider the **national age limit** for children giving consent on their own or with their parents. The UNCRC recognised the child's basic right:

- **For their views to be sought and respected:** Every child has the right to express their views, feelings and wishes in all matters affecting them, and to have their views considered and taken seriously.
- **To receive information and to express themselves freely:** children have the basic right to information in ways that are appropriate for their developmental level so that they can form and freely express their opinion.

- **For their evolving capacities to be taken into account:** while parents and carers are recognised as the responsible people to provide guidance and direction to their child as they grow up, this must be done in a way that recognises the child's increasing capacity to make their own choices.

Schools must ensure that consent by children and consent by parents is:

- **Freely given,** without feeling pressure,
- **Specific and informed,** understanding the purpose of collecting data,
- **Unambiguous,**
- **Easily withdrawable** at any time.

Parental or guardian consent – verifying the consent/ assent of the child – is typically required for children under the age of **16** (or lower, depending on national laws).

Schools should:

- **Explain Data Usage Clearly:** Provide explanations that are both age-appropriate and consider parents' literacy levels of data collection, use store and sharing, and their implications.
- **Seek Assent for Children:** Even when parental consent is required, children should be given the opportunity to express their views and preferences.
- **Respect the Child's Wishes:** If a child objects to the use of their data (such as photo sharing, it must be respected.

Sharing Photos and Videos Publicly: Special Considerations

One of the most sensitive areas of data protection in schools relates to the sharing of student images and videos. Schools often wish to highlight student achievements, promote events, and share community engagement on websites, social media, and newsletters. But the reality is that researchers have found that 70% of pictures of children shared publicly end up on the dark web and abused by sexual predators.

Therefore, the following guidelines must be followed:

1. **Obtain Explicit Consent:** Before sharing any identifiable photos or videos of students, explicit child and parental consent is required. This should be a separate consent from general school agreements.
2. **Use Secure Platforms:** If sharing internally, use secure school portals instead of public social media.
3. **Blur or Anonymize Faces:** If sharing photos publicly, consider blurring faces or avoiding direct identification.
4. **Avoid Tagging Students:** Never include full names or any identifying details in publicly shared photos.
5. **Restrict Access:** If sharing within a school network, limit access to authorized personnel only.
6. **Regularly Review Permissions:** Ensure that consent forms are updated whenever new photos/videos are to be shared, and also allowing students and parents to modify or withdraw permissions.

Challenges and Best Practices:

- **No blanket consent obtained beforehand**: Following the principles of evolving capacities and providing information that is understandable for children, blanket consent, especially if asked for beforehand, must be avoided.
- **The role of the Data Protection Officer (DPO):** It is compulsory to appoint a dedicated person responsible for ensuring GDPR compliance in the school. Everybody, even children on their own should be able to approach this person. Complaints must be taken and acted upon seriously.
- **Training Staff:** Teachers and administrative staff should receive regular training on data protection responsibilities as well as compliant activities e.g. in photo and video use.
- **Clear Communication:** Providing parents with detailed privacy policies in accessible language.
- **Incident Management:** Establishing a clear protocol for handling data breaches or complaints related to data privacy.
- **Engaging with Students:** Educating older students about their data rights and how they can exercise them.

In conclusion, GDPR and the UNCRC ensure that children's data rights are respected in educational settings. School leaders play a crucial role in enforcing these standards through responsible data collection, transparent consent procedures, and cautious handling of multimedia content. By integrating best practices into daily school operations, school leaders can foster a secure and legally compliant environment that protects students' privacy while enabling educational development.