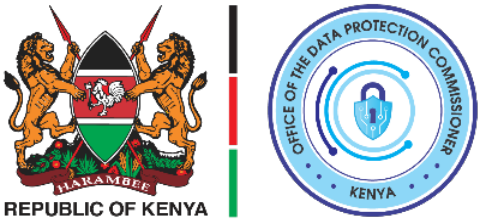

OFFICE OF THE DATA PROTECTION COMMISSIONER

Guidance Notes for Processing Children's Data

2025

TABLE OF CONTENTS

FOREWORD

The rapid adoption of digital technologies in education, health, entertainment, and social interactions has created both opportunities and risks for children. Children are among the most vulnerable members of our society. Protecting their right to privacy and personal data is crucial because mishandling it can result in risks that last a lifetime—such as identity theft, profiling, online exploitation, and discrimination. Therefore, the Constitution of Kenya 2010, the Children's Act 2022, and the Data Protection Act 2019 collectively safeguard the right to privacy and the principle that the best interests of the child are paramount in all matters concerning them.

While digital platforms can enhance learning and foster creativity, they can also endanger children's dignity and well-being if their personal data is handled without sufficient safeguards. Unlike adults, children might not fully understand the consequences of sharing their personal information, which increases the responsibility of data controllers, processors, and service providers to always act in their best interests.

Consequently, the Office of the Data Commissioner (Office), in its mandate to protect and regulate the processing of children's personal data, developed this Guidance Note to clarify the obligations of organisations in both the public and private sectors that process children's data. It emphasises the legal and ethical duty to obtain verifiable parental or guardian consent, encourages the development and implementation of practical age-verification mechanisms, and the adoption of robust technical and organisational safeguards. It also emphasises the importance of privacy by design and default, data minimisation, secure data retention, and conducting Data Protection Impact Assessments where high-risk processing occurs.

The Office reaffirms that children's personal data must never be treated as a commodity. Instead, it must be processed lawfully, fairly, and transparently, primarily to protect their rights to privacy, safety, and development. The aim of simplifying the Act and its regulations in this Guidance Note is to offer guidance to those processing children's personal data on their legal but also moral obligations in ensuring that children can safely participate in and benefit from the digital society without harm.

My hope is that data handlers will progressively implement the principles of data protection in safeguarding the dignity and future of Kenya's children. By doing so, we collectively reaffirm our national commitment to protecting the rights of every child in the digital age.

Immaculate Kassait**, MBS**
Data Commissioner

1. DEFINITIONS

"**Abuse**" means misuse of a child's personal data, such as exploiting their data for harmful purposes like identity theft, profiling, or exposure to harmful content online.

"**Act**" means the Data Protection Act, No 24. of 2019.

"Anonymization" means the permanent and irreversible removal of personal identifiers from personal data so that the data subject is no longer identifiable.

"Best Interest" means the principles that prime the child's right to survival, protection, participation and development above other considerations and includes the rights contemplated under Article 53 (1) of the Constitution and section 8 of the Children's Act.

"Child" means an individual who has not attained the age of eighteen years.

"**Child Protection**" Means specific safeguards applied to ensure that children's data is processed in a way that prioritizes their safety, privacy, and well-being.

"Consent" means any manifestation of express, unequivocal, free, specific, and informed indication of the data subject's wishes by a statement or by clear affirmative action, signifying agreement to the processing of personal data relating to a data subject. For children, this specifically entails explicit permission given by a parent or legal guardian in accordance with this Guidance Note.

"Data Controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of Processing of Personal Data;

"Data Handlers" means a data controller and or data processor.

"Data Processor" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.

"Data Subject" means an identified or identifiable natural person who is the subject of Personal Data.

"Encryption" means the process of converting the content of any readable data into an unreadable format using technical means to protect it from unauthorized access.

"**Guardian**" means a person appointed by a parent, court, or a legal authority to take responsibility for a child's welfare, including legal, physical, and emotional care.

"**Parent**" means a biological, adoptive, or step-parent of a child.

"**Parental/ guardian consent**" means explicit permission given by a parent or legal guardian on behalf of a child (an individual under 18 years) for the processing of the child's personal data.

"**Processing**" means any operation or sets of operations which is performed on personal data

or on sets of personal data whether or not by automated means, such as

(a) collection, recording, organisation, structuring;

(b) storage, adaptation or alteration;

(c) retrieval, consultation or use;

(d) disclosure by transmission, dissemination, or otherwise making available; or

(e) alignment or combination, restriction, erasure or destruction.

"Pseudonymization" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, and such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

"**Regulations**" means practical framework that operationalizes the principles outlined in the Data Protection Act, including the Data Protection (General) Regulations, 2021.

2. THE OFFICE

The Office of the Data Protection Commissioner is a government agency established to protect the privacy and security of personal data in our increasingly digital world. It has the responsibility of enforcing data protection laws and policies to safeguard the privacy, dignity, and fundamental rights of individuals. The office is mandated to oversee the implementation and enforcement of the Act, which regulates the processing of personal data of persons located in Kenya by both private and public sector organisations.

The Office plays a vital role in ensuring that individuals control their personal data and that organisations respect their privacy rights. The Office's work involves monitoring and enforcing compliance with data protection regulations, investigating data breaches and imposing sanctions on entities that violate data protection laws. In addition, the office is responsible for raising public awareness about data protection issues and educating individuals and organisations on how to protect personal data. With the growing importance of data protection in our digital age, the Office is a critical institution in maintaining trust and confidence in our data-driven society.

The Office is uniquely positioned to facilitate both the government and private sector entities in achieving the Government's strategic goals under the "Bottom-Up Economic Transformation Agenda" and specifically its digital superhighway initiative. As the digital landscape expands, the need for robust data protection mechanisms becomes paramount. The Office, in its mandate to oversee, regulate, and ensure lawful data processing, plays a pivotal role in this transformation. Kenya remains at the cutting edge of digital transformation while maintaining stringent data protection standards. The Office serves as a key stakeholder and regulator in guiding the nation's digital superhighway journey by ensuring that as we advance technologically, the rights and privacy of individuals remain safeguarded.

3. INTRODUCTION

Proper handling of children's personal data is crucial due to their inherent vulnerability and limited capacity to fully understand the implication of the processing of the personal data. Additionally, children might not be able to understand the long-term risks connected to the processing of their personal data. When processing children's sensitive data, such as race, health status, ethnic social origin, conscience, belief, genetics, and biometrics, data handlers need to adhere to data protection principles and include additional safeguards. Maintaining the confidentiality and integrity of children's data is essential to upholding their right to privacy and the organisations' reputation.

Children's data is increasingly being processed and stored online due to the advancement of technology and adoption of digital platforms, making it susceptible to unauthorized access, cyberattacks, and data breaches. Although many aspects of learning and development can benefit from these technologies, concerns arise regarding the protection of children's privacy. Entities processing children's data must put in place adequate safeguards to mitigate the risk that the data will be misused or accessed by malicious individuals.

The Act offers the legal foundation for guaranteeing that personal data, including children's data, is managed in a legal, equitable, and safe manner. In Kenya, the right to privacy is protected by the Constitution. This law requires that institutions and organisations that process children's data follow certain requirements, including establishing a lawful basis for processing, obtaining parental or guardian consent/authorization as a safeguard, ensuring the data is accurate, and implementing adequate security measures. Since children might not completely comprehend the implications of data sharing, these precautions are especially important for their protection.

The necessity to put children's best interests first while processing their data is a fundamental premise. This entails keeping data collection at a minimum, safeguarding it against unwanted access, and maintaining openness regarding the data's collection and use. Obtaining consent from a parent or guardian is crucial for organisations, as children generally lack the legal capacity to provide consent on their own. In addition, it's critical to put in place procedures that let parents quickly view their children's data and revoke their consent.

In conclusion, a proactive and cautious approach is needed to secure children's personal data. Organisations processing such data must have procedures that not only abide by the Act but also protect children's rights and welfare, since children are especially susceptible to data misuse. We can shield minors from invasions of privacy and guarantee the security of their personal data by making sure that data is handled securely and openly.

4. PRIVACY CONCERNS

Children are more vulnerable to privacy violations because they are less able to fully comprehend their digital rights and are frequently ignorant of the repercussions of data collecting. To protect children's privacy, data controllers, service providers, and other organisations that handle children personal data need to exercise extra caution and make sure that the necessary security measures are in place. When children's data is misused, it can result in serious issues that can negatively affect their wellbeing for a long time, like identity theft, profiling, and unauthorized data sharing.

The lack of transparency surrounding the collection and use of children's data is a major worry, particularly when it comes to digital platforms and services. Numerous personal data, including behavioural, location, and health information, may be gathered by applications and websites, frequently without the explicit or informed consent of minors or their guardians. Children are often left open to exploitation or improper data usage because parents or guardians may not completely comprehend the scope of data gathering and processing. Service providers need to make sure that children and their guardians are properly informed about their data practices and that appropriate consent is acquired.

Another major concern is the vulnerability of children's personal data to cyber-attacks and data breaches. Children's data is becoming a more appealing target for cybercriminals as more businesses and platforms cater to them. Due to a lack of strong cybersecurity safeguards, many organisations managing this data may be vulnerable to hackers, breaches, or unauthorized access. Identity theft, fraud, or the selling of personal data to unaffiliated third parties are all possible outcomes of breaches affecting children's data. Encryption and strong cybersecurity policies are needed to protect children's private information and stop illegal access.

Another urgent concern is the exploitation of children's data for predictive analysis and profiling. Such actions may have a significant impact on a child's future in terms of resources, opportunities, and services available to them. Behaviour, health, or socioeconomic background-based profiling can result in unjust exclusion or discrimination, which can have an adverse effect on a child's long-term development. To guarantee that no child is exposed to prejudice or long-term injury because of data-driven decision-making processes, it is imperative that any processing of children's data be done fairly and ethically.

Finally, there are issues with tracking children's activities via surveillance technologies such as CCTV. Even while these technologies are frequently introduced for safety reasons, if they are used excessively or without a good reason, they may violate children's right to privacy. Children who are constantly watched over may grow up in situations of mistrust and restriction, which will limit their freedom to experiment and express themselves. The protection of children's privacy must be carefully balanced with the need to ensure their safety. Any use of surveillance techniques must be proportionate, open, and supported by the necessary safeguards.

5. SCOPE & PURPOSE

In exercise of the powers of the Data Commissioner pursuant to the Act and the Regulations, this Guidance Note provides for considerations that must be present when processing children's personal data. The guidance note provides:

a) A distinction between consent as a lawful basis and parental or guardian consent
b) Application of key data protection principles
c) Privacy concerns while processing children's data
d) Child data protection considerations
e) Exercise of Children's rights
f) Obligations of Data Controllers and processors while processing Children's data

This guidance note considers:

a) The Constitution of Kenya, 2010;
b) The Data Protection Act, 2019;
c) The Data Protection Regulations;
d) Other applicable laws and regulations; and
e) International Best Practice.

This Guidance Note applies to data handlers in either the public or private sectors who process children's data.

6. LEGISLATIVE FRAMEWORK

The processing of children's personal data is guided by the following legislative framework:

a) The Constitution of Kenya 2010

Article 31 (c) and (d) guarantees the right to privacy and provides that every person, has the right not to have information relating to their family or private affairs unnecessarily required or revealed, or to have the privacy of their communication infringed.
Article 53 (2) provides that a child's best interests are of paramount importance in every matter concerning the child.

b) The Children's Act of 2022

Section 8(1) of the Children Act underscores that in all matters concerning children, the best interests of the child shall be a primary consideration. This principle serves as a guiding standard for any data processing activity involving children.

Furthermore, Section 27 affirms a child's right to privacy, requiring that a child shall not be subjected to arbitrary or unlawful interference with their privacy, family life, private affairs, correspondence, or to attacks on their honour or reputation.

These provisions collectively emphasize the need for heightened safeguards and ethical considerations when handling children's personal data.

c) The Data Protection Act, 2019 (and attendant Regulations)

The Act specifies the requirements and considerations data handlers must consider when processing personal data relating to children.

7. APPLICATION OF DATA PROTECTION PRINCIPLES

Processing of children's personal data should be done in accordance with the principles of data protection set out in section 25 of the Act with a heightened emphasis on the best interests of the child, recognizing their vulnerability and limited capacity to understand data processing implications. A data handler processing children's data should ensure that there is:

a) a lawful basis for processing and for personal data relating to a child, parental or guardian consent;
b) fairness in the processing and a parent or guardian is informed of the inherent risks in the processing;
c) a legitimate, explicit and specific purpose for processing;
d) a mechanism for limiting collection to only what is necessary in relation to the purposes for which it is processed;
e) measures for ensuring accuracy of the personal data;
f) A procedure for deleting or anonymising personal data that is no longer needed;
g) Technical and organisational safeguards for ensuring security of personal data; and
h) Adequate safeguards for transfer or consent of the parent or guardian.

The Office has published sector specific guidance notes which comprehensively address the principles of data protection. Still, this guidance note explores all key data protection principles in relation to processing children's data.

7.1 Lawfulness, fairness, and transparency

Personal data collected about children must be processed in a lawful, fair, and transparent manner. For lawful processing, data handlers are required to process personal data in accordance with the law by identifying a legal basis for the processing. This could include obtaining consent from parents or guardians, protecting the vital interests of the child, exercising official authority, or pursuing legitimate interests, amongst others.

Data handlers must ensure that the processing of personal data is fair and considers the best interests of a child. This involves being transparent about how the collected data is processed and making sure that children and their legal representatives are aware of their rights.

7.2 Purpose Limitation

The processing of children's data must be for a specific, explicit and legitimate purpose and not repurposed without a clear legal basis and consent. The processing activity should be in the best interest of a child. Regulation 13 of the General Regulations prohibits data handlers from profiling a child in relation to direct marketing.
Parents or guardians should be made aware of the purpose of the processing activities and data handlers should seek additional consent if the data is used for a new purpose.

7.3 Data Minimization

Data minimisation is a critical aspect of data protection especially when processing children's data. The principle requires that personal data collected and processed is relevant and limited to what is necessary for the purpose identified. Only collect the categories and types of data necessary for the specific purpose.
Data handlers should evaluate the specific types of data required and avoid broad or unnecessary data collection. For example, an online learning platform designed for children does not need to have the full name of the child while they can rely on a unique identifier.

7.4 Accuracy

The personal data collected about children must be accurate and kept updated, with necessary steps being taken to ensure that inaccurate data is erased or rectified. To comply with this principle, as part of their data management, data handlers should implement clear procedures enabling prompt detection/reporting of inaccuracies, correction, or erasure of any inaccurate personal data.

7.5 Storage Limitation

This principle is to the effect that personal data identifying children should only be kept for as long as necessary and solely for the purposes for which it was collected. Children's personal data must be reviewed regularly, and it should be erased or anonymized once it is no longer needed.

7.6 Integrity and Confidentiality

This principle requires that personal data be processed in a manner that ensures its security. This includes protection against unauthorized or unlawful processing, as well as safeguards against accidental loss, destruction, or damage.

Confidentiality and data security are essential aspects of data protection, especially given the sensitivity and volume of personal data collected about children. Therefore, all technical procedures used to process children's data should incorporate strong security measures, with clearly defined standards in place.

7.7 Accountability

The principle of accountability emphasizes responsible data handling practices, compliance with legal requirements, and respect for the rights of data subjects. This involves taking proactive steps to protect personal data. While processing children's data, data handlers should put in place measures such as:

a) Adequately informing the parent or guardian of the inherent risks in processing in line with the principle of transparency.
b) Establishing an appropriate lawful basis for processing children's data

c) Obtaining verifiable parental or guardian consent.
d) Implementing age verification mechanisms.
e) Implementing technical and organisational safeguards for ensuring confidentiality and integrity of data.
f) Providing mechanisms for parents or guardians to exercise the rights of the data subject who is a minor.
g) Instituting procedures for conducting due diligence and audits of third-parties data handling practices.
h) Employee training and awareness.
i) Regular data compliance audits.
j) Conducting a Data Protection Impact Assessment (DPIA) to identify potential risks that can be mitigated prior to the commencement of processing.
k) Parents and guardians can also be reassured that the organisation has taken careful steps to protect their children's data.

Example:

Qusoma educational app for children collects data to personalize learning experiences and track progress. It gathers personal information like name, age, and grade level, along with learning data such as quiz scores and usage patterns. Before collecting any data, the app verifies the child's age and requires parental consent, providing clear explanations about data use and access.

The app personalizes content based on individual learning needs, generates progress reports for parents, and ensures data security through encryption and limited access. Data is retained only as long as necessary for educational purposes, and parents can request deletion at any time. The app also keeps parents informed about their child's progress, fostering trust and collaboration.

8. LAWFUL BASIS VS PARENTAL/GUARDIAN CONSENT

The Act provides for eight lawful bases for processing personal data. Section 30 of the Act requires that personal data must only be processed if at least one of the legal grounds listed in that section applies. A data handler processing personal data may rely on either of the basis, including but not limited to legal obligation, performance of a public task carried out by a public authority, performance of a contract, legitimate interests, or consent.

The Act defines consent as any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action. Therefore, for consent to be valid, it ought to be specific, informed and freely given. The Act places the responsibility of demonstrating that valid consent was obtained on the data handler. Additionally, when processing personal data relating to children, Section 33 of the Act stipulates that consent should be given by the child's parent or guardian, and the processing should be in a manner that protects and advances the rights and best interests of the child. In all cases of data collection especially online, a data handler must incorporate appropriate mechanisms for age verification take reasonable efforts to verify that consent is given by the parent or guardian, taking into consideration available technology.

Example 1:

A school plans to celebrate a student's top academic performance by publishing their name, photograph, and scores on its website and social media. Since this is not necessary for the child's education, the school must rely on **consent as the lawful basis** for processing the student's personal data. This means that the school must obtain clear, informed, and voluntary approval before using the child's information. However, because the student is a minor, they may not have the legal capacity to provide valid consent on their own. In such cases, parental consent is required before any data processing takes place. Consent must be specific to the intended use, ensuring that the parent or guardian understands how the data will be shared and has the option to decline.The school must verify the identity of the parent or guardian, ensuring that the consent is legitimate and properly documented. While **consent as a lawful basis justifies the processing of personal data, parental consent is a procedural safeguard** ensuring that decisions regarding a child's data are made by someone with legal responsibility for their well-being. Without verified parental consent, the school cannot proceed with publishing the student's information.

Example 2:

Before collecting any data for a child's passport application, the immigration authority must ensure that the lawful basis for processing is clearly established, primarily compliance with a legal obligation and the exercise of official authority. Since the applicant is a minor, parental or guardian consent must be obtained before data collection begins. The parent or guardian must provide proof of relationship, such as a birth certificate or guardianship order, and sign a consent form confirming their approval. The authority must also inform them of how the child's data will be used, stored, and shared, ensuring transparency and security safeguards to protect the child's personal information.

Regardless of the legal basis relied upon by the data handler, parental consent must be obtained when processing children's data. Where other lawful bases for processing a child's personal data are applicable, parental or guardian consent primarily serves as a means of fulfilling the notification obligation, rather than functioning as the primary legal basis for processing.

In such cases, this form of consent is not equivalent to consent as a lawful basis under the Data Protection Act and therefore may not carry the same implications such as the right of withdrawal associated with consent used as a standalone legal basis. It is essential to recognise the distinction between consent as a lawful basis for processing and parental or guardian consent.

Where a data handler is processing a child's personal data, it is required that the data handler identify a clear and justifiable legal basis and in addition to identifying this basis, the data handler must also obtain explicit consent from the child's parent or guardian before collecting or processing the child's personal data.

Example:

An insurance fund established by an Act of Parliament requires that all residents in the country register as members of the fund. The targeted individuals will include children in the country. The processing the personal data of the citizens, the fund will rely on its legal obligation to process personal data for the provision of health insurance in Kenya. In addition, to process children's data, the fund must obtain parental or guardian consent and have a mechanism for age verification and verifying the parental or guardianship relationship.

9. CHILD DATA PROTECTION CONSIDERATIONS

9.1. Best Interest of the Child Principle

Section 2 of the Children Act, 2022, defines the best interest of the child as the principles that prime the child's right to survival, protection, participation and development above other considerations and includes the rights contemplated under Article 53 (1) of the Constitution and Section 8 of the Children Act.

Article 53(2) of the Constitution and Section 8 of the Children Act emphasise that the child's best interests are of paramount importance in every matter concerning the child. Therefore, all persons, when exercising any powers conferred under any law, including processing of personal data for children shall treat the best interests of the child as the first and paramount consideration to the extent that is consistent with adopting a course of action calculated to: -

(a) safeguard and promote the rights and welfare of the child;
(b) conserve and promote the welfare of the child; and
(c) secure for the child such guidance and correction as is necessary for the welfare of the child and in the public interest.

Placing the best interests of the child as a primary consideration recognises that the child's best interest is flexible and adaptable. It should be adapted and defined on an individual child basis, according to the specific situation of the child concerned, considering their personal context, situation and needs.

The Constitution, Children Act, and the Data Protection Act do not expound on what constitutes the best interest of a child. However, the first schedule of the Children Act provides a list of the best interest considerations which all data handlers should consider when dealing with a child's data. Generally, a data handler should consider, among other things how, in the use of personal data of a child, they can: -

i. recognise the role of parents in protecting and promoting the best interests of the child and support them in this task;
ii. keep them safe from any form of exploitation risks, including data specific exploitation such as unauthorised profiling, targeted advertising, or misuse of personal information.
iii. protect and support their physical, psychological and emotional development;
iv. protect and support their need to develop their own views and identity;
v. support the needs of children with disabilities and;
vi. recognise the evolving capacity of the child to form their own view and give due weight to that view.

Therefore, in determining what the best interest of the child is a data handler needs to assess

the following before processing children's data: -

i. Understand the rights of the child by considering how the processing of the child's data could positively support or pose risks to these rights.
ii. Identify impacts. An effective children's best interest's assessment requires a detailed and nuanced understanding of how, why and when a data handler's activities involve processing of children's data. You also need to be aware of the activity features that shape how children and parents engage with this processing, to ensure a data handler conforms with the standards within the Act. An understanding of these two areas lays the groundwork for a data handler to identify how its activities can risk, or support, children's rights and best interests.
iii. Assess impacts: Next step after identifying the potential impacts of the processing on the rights of a child, a data controller and/or processor must assess the likelihood of these impacts occurring, and the magnitude of these impacts on children if they occur.
iv. Prioritize actions: After the data controller and/or processor has assessed the extent of the impact of the processing on children's rights a data handler should create an action plan for addressing the risk areas highlighted in the risk assessment and deliver an action plan for upholding children's rights.
v. To assist data handlers in carrying out this assessment of the best interest principle, entities are required to conduct a DPIA to assist them assess the risks posed by the processing of children's data.

It is only after establishing that the processing is in the best interest of the child that a data handler should move to the next step of obtaining parental consent.

9.2. Parental or Guardian consent

The Children Act of 2022 defines a child as anyone under the age of 18 years. Consequently, the age of consent is 18 years. Processing of data relating to a child is prohibited under the Act unless verifiable informed consent is given by the child's parent or guardian, making parental consent a cornerstone in safeguarding children's rights and the right to privacy.

For parental consent to be informed, it is the holder of parental responsibility rather than the child who needs to understand what they are consenting to. Providing clear privacy information should meet this requirement. A data handler is required to inform the parent of the following before seeking parental consent:

(a) the identity of the data controller or data processor;
(b) the purpose of each of the processing operations for which consent is sought;
(c) the type of the personal data that is collected and used;
(d) information about the use of the child's personal data for automated decision-making where relevant and provision of human intervention;

(e) whether the personal data processed shall be shared with third parties.

In addition, the provision of this parental consent must not be marred by any illusion of choice, nor should there be adverse consequences for parents who choose not to provide their consent. Data handlers must also provide an easy mechanism for withdrawing the consent given. Typically, the withdrawal of consent should be possible to achieve through the same means used to give consent.

9.3. Verification of Authority of Parents or Guardians

It is important to verify the authority of parents or guardians to ensure that the parental consent is genuine. It is also important to ensure that the person giving consent is the child's parent or guardian, and not an imposter. Verification can be done in a variety of ways, such as by requiring a signed consent form, email verification, checking government-issued identification documents, use of third-party verification services or using electronic signatures. This process must be an acceptable and proportionate verification approach as well as compliant with the principle of data minimization.

9.4. Age verification

In processing personal data relating to a child, age verification is an important tool for protecting children's data. Age verification ensures that children access appropriate services and content that is not harmful to them. Age verification online allows age-appropriate data protection mechanisms adapted to age ranges of all children. Examples of age verification methods include requiring users to enter their date of birth, using identity documents, implementing age gates or conducting age checks with a secure third-party service. Age verification alone may not prevent children from being exposed to online harm. However, all methods of age verification must be proportionate, privacy preserving and adhere to the principle of data minimization.

9.5. Mechanisms for Age Verification & Obtaining Consent

To process personal data of a child, a data handler shall incorporate appropriate mechanisms for age verification and consent which shall be determined based on:

a) available technology;
b) volume of personal data processed;
c) proportion of such personal data likely to be that of a child;
d) possibility of harm to a child arising out of processing of personal data; and
e) such other factors as may be specified by the Data Commissioner.

The mechanisms are likely to vary from context to context, however they should be

proportionate and grounded on a risk-based approach. This means that there should be greater stringency or levels of certainty provided by the verification process where the processing of personal data undertaken by a data handler is of higher risk. In addition, age verification and consent mechanisms developed and utilized by data handlers must comply with the obligation of data protection by design and default and must also be subjected to data protection impact assessments to assess whether the mechanism in question complies with the principles of data protection and data security.

Example:

When a user attempts to register an account, they are asked for their date of birth. If the user indicates that they are under 18 years, they are notified that parental/guardian consent is required to proceed. The platform sends an email to the provided parent/guardian's email address with a link to a consent form. To ensure the person providing consent is an actual parent or guardian, the platform may require submission of official documents such as an ID. The parent or guardian is informed about the nature of the data being collected, how it will be used, and the rights they have regarding the collected data. The parent or guardian must actively agree to the processing of the minor's personal data by checking boxes or signing digitally. Once the system logs the consent, the user can continue with the standard process of account registration.

9.6. Exercise of Children's rights

Regulation 13 of the Data Protection (General) Regulations emphasize that where a child is involved, the rights to access, rectify, restrict, or delete personal data should be handled by a parent or legal guardian. These rights should be exercised in the best interest of the child, ensuring that the child's data is protected and used appropriately. Data handlers must ensure that parents or guardians are appropriately identified when making requests on behalf of their children. In addition, direct marketing activities targeting children and profiling, are prohibited to prevent exploitation of their data.

9.7. Exemption to Parental consent

Section 33(4) of the Act provides that a data controller or data processor that exclusively provides counselling or child protection services to a child may not be required to obtain parental consent. In cases where the parent or guardian has abandoned the child, neglected them, or unreasonably withheld consent, the data handler is encouraged to ensure the best interest of the child as provided for in Article 53 of the constitution.

10. SAFEGUARDS FOR PROCESSING CHILDREN'S DATA

It is vital to implement robust safeguards to ensure that children's personal data is protected at all stages of processing. Below is a set of guidance to help data controllers and processors comply with these requirements when handling children's data, both manually and digitally.

10.1. Security Measures

(a) Manual Data Processing Safeguards:
   i) Store manual records such as paper files containing children's data in secure locations (locked cabinets, restricted access areas).
   ii) Limit physical access to the data to authorized personnel only.
   iii) Establish clear policies for safe disposal of manual records, including shredding or secure destruction.

(b) Digital Data Processing Safeguards:
   i) Use encryption and pseudonymization to protect children's data during storage and transmission.
   ii) Implement role-based access controls to ensure that only personnel with legitimate authority can access children's data.
   iii) Ensure multi-factor authentication and strong password protection for systems handling children's data.
   iv) Regularly audit and monitor systems for security vulnerabilities and breaches based on the latest cybersecurity best practices and emerging threat intelligence, emphasising continuous risk assessment and adaptation.

10.2. Data Retention Policies

(a) Retain children's personal data only for as long as necessary to fulfil the processing purpose.
(b) Create a data retention schedule that outlines specific periods for retaining children's data.
(c) Ensure personal data is securely deleted or anonymized when no longer required for the stated purpose.

10.3. Parental/Guardian Consent

(a) Before collecting personal data from children, obtain explicit consent from parents or guardians, regardless of the sensitivity of data collected.
(b) Use simple and clear consent forms tailored to parents and children, outlining the nature of the data, purpose of processing, and rights. Obtain new consent if data processing activities change or expand.

10.4. Staff Training and Awareness

(a) Ensure that all personnel handling children's data are trained on data protection principles and best practices for safeguarding sensitive data.

(b) Conduct regular training sessions on privacy principles, including the specific vulnerabilities and risks associated with children's data. Implement clear internal policies regarding access, processing, and secure disposal of children's personal data.

10.5. Accountability and Audits

(a) Establish clear accountability mechanisms to ensure that the entity is responsible for the protection of children's data at all stages of processing.
(b) Conduct regular internal audits to monitor compliance with data protection laws.
(c) Designate a Data Protection Officer (DPO) or data protection committee responsible for overseeing the processing of children's data and ensuring compliance with legal and regulatory requirements.

10.6. Data Breach Notification

(a) In case of a data breach, promptly notify the Office and parents/guardians, particularly if the breach affects children's personal data.
(b) Establish a data breach response plan that details how to detect, respond to, and communicate breaches. Notify affected individuals without undue delay and take immediate action to mitigate further harm.

11. OBLIGATIONS OF DATA CONTROLLERS AND PROCESSORS IN PROCESSING CHILDREN'S DATA

11.1. PROCESSING OF SENSITIVE PERSONAL DATA OF CHILDREN

The processing of sensitive personal data of children is common in various sectors, including healthcare, education, social services, and digital platforms. Entities that process children's data must ensure compliance with the law, as sensitive personal data requires a higher level of protection to safeguard the privacy rights of child data subjects. Sensitive personal data is a category of personal data that, due to its nature, demands stricter protections, as its processing can significantly impact the privacy and rights of children.

Sensitive personal data includes information such as a child's health, biometric data, ethnicity, religious beliefs, and any other information that could pose significant risks to a child's rights and freedoms if mishandled, this could significantly impact their rights, freedoms, or well-being.

When handling children's sensitive data, data controllers and processors must meet certain conditions laid out in the data protection laws, including obtaining explicit parental consent or ensuring that the processing is necessary for the performance of a legal obligation or for other enumerated lawful bases.

Guidance:

(a) **Identify Lawful Basis and Purpose:** Before collecting and processing sensitive personal data, entities handling children's data must identify a lawful basis and a clear and legitimate purpose for the processing. Sensitive personal data should only be processed where there is a specific lawful basis such as explicit consent, legal obligations, or protection of the child's vital interests. For instance, healthcare providers may process health data of children to protect their well-being or in response to a medical emergency under the vital interest lawful basis.

(b) **Obtain Explicit Parental Consent:** Before processing sensitive personal data, entities must obtain explicit parental or guardian consent. This means that the parent or guardian must provide clear, unambiguous, and specific consent for their child's sensitive data to be processed. For example, if a platform collects biometric data from children, explicit consent from parents must be secured before any data processing takes place.

(c) **Processing Based on Legal Obligations:** In some situations, entities may be required to process sensitive personal data of children to fulfil a legal obligation. In such cases, the data handler must ensure that the processing is necessary for compliance with the legal requirement. For instance, schools may be required to process health or disability data to comply with regulatory requirements or public health mandates.

(d) **Vital Interests or Legal Claims:** Processing sensitive personal data may also be necessary to protect the vital interests of the child or another individual. This could include life-saving medical treatment or emergency care. Additionally, processing may be necessary for the establishment, exercise, or defence of legal claims in cases involving children's rights or safety.

(e) **Implement Security Measures:** Entities that process sensitive personal data of children must take appropriate technical and organisational measures to ensure data security. For

example, only authorized personnel, such as a doctor or therapist, should have access to a child's health records, which should be kept confidential. Security measures should include encryption, pseudonymization, and access controls to protect the data from unauthorized access or misuse.

(f) **Retention Periods:** Sensitive personal data of children should be retained only for the period necessary to achieve the processing purpose. Once the data is no longer required, it should be securely deleted or anonymized. For example, after a medical condition has been treated, the health data should be deleted unless there is a legal reason to retain it.

(g) **Cross border Data Transfer:** Transfer of children data should meet the general conditions of cross border data transfer under section 48.

11.2. Privacy by Default or Design

The Act, specifically in Section 41, mandates that entities processing children's personal data must implement appropriate technical and organisational measures to ensure effective adherence to data protection principles. This includes establishing necessary safeguards throughout the data processing lifecycle. Notably, the act stipulates that only the minimum necessary children's personal data should be processed. This consideration encompasses the amount of data collected, the extent of its processing, the duration of storage, accessibility, and the cost associated with processing.

Privacy by Design is a proactive approach requiring data controllers and processors to incorporate privacy and data protection considerations from the very start of any system, service, product, or process development. This means evaluating and addressing potential privacy risks during the design phase and maintaining this focus throughout the data lifecycle. Privacy by default complements this approach by ensuring that only the data necessary for achieving a specific purpose is processed. This requires entities to:

(a) **Limit Data Collection**: Clearly specify the personal data needed before initiating any processing activities.

(b) **Inform Stakeholders**: Appropriately inform children and their parents or guardians about the data being collected and its intended use.

(c) **Minimise Data Use:** Only process personal data essential for fulfilling the stated purpose, avoiding unnecessary data collection.

Incorporating these principles ensures that processes involving sensitive data are designed with the child's best interests at heart, prioritising their privacy and protection.

11.2.1. Building Public Trust

Adherence to the principles of data protection by design and by default is crucial for building public trust. When entities demonstrate a commitment to safeguarding children's data, it fosters confidence among parents and guardians regarding how their children's personal information is handled.

11.2.2. Cost-Benefit Perspective

Implementing data protection by design and default is also a wise decision from a cost-benefit perspective. Integrating privacy measures at the onset can significantly reduce the need for costly adjustments or retrofitting later. Modifying existing processing operations to enhance privacy can be complex and expensive, making proactive compliance more efficient and effective.

12. DATA PROTECTION IMPACT ASSESSMENT

Before processing any sensitive personal data relating to children, data handlers must conduct a Data Protection Impact Assessment (DPIA) under Section 31 of the act, especially if the processing is likely to result in a high risk to the child's rights and freedoms. DPIAs are necessary when processing children 's data due to the following:

12.1 High-Risk Data Processing

Children are considered vulnerable data subjects due to their limited capacity to understand the complexities of data processing. Certain processing activities involving children's data, especially sensitive personal data such as health, biometric, or location data, carry a high risk to their privacy. A DPIA is required when such processing is likely to result in high risks to children's rights and freedoms, such as identity theft, tracking, profiling, or potential data breaches.

12.2 Special Protections for Children's Data

Children have heightened privacy protections under the law, including requirements for explicit parental consent and the best interests of the child principle. A DPIA helps ensure that all special protections are respected by identifying areas where additional safeguards are necessary.

12.3 Identifying and Minimizing Risks

DPIAs assist data handlers in assessing risks and developing measures to mitigate them. These risks might include unauthorized access, misuse of sensitive data, profiling for marketing purposes, or data breaches. By conducting a DPIA, organisations can identify these risks early and implement measures to minimise or eliminate them.

12.4 Ensuring Compliance with Data Protection Laws

Under the Act, organisations must process children's data in a way that complies with the law. DPIAs help ensure that data protection principles, such as data minimisation, purpose limitation, and integrity, are integrated into processing activities from the outset. This proactive approach helps prevent potential legal issues and penalties, as well as damage to the organisation's reputation.

12.5 Proactive Privacy by Design and Default

DPIAs support the implementation of privacy by design and by default principles by ensuring that privacy risks are addressed during the design of systems and processes that handle children's data. This ensures that data protection is embedded into every step of the data processing lifecycle, from collection to storage and deletion.

12.6. Preventing Harm to Children

Processing children's data without proper safeguards can lead to serious consequences, such as exploitation, psychological harm, or physical danger, especially when location data is misused. DPIAs help to foresee and prevent such risks by identifying the measures that should be in place to protect children's privacy and safety.

In addition to the aforesaid, the Act requires that all data controllers and processors implement appropriate technical and organisational measures and integrate appropriate safeguards to ensure the adequate protection of the personal data of data subjects.

The Office has published a Guidance Note on Data Protection Impact Assessments on www.odpc.go.ke The guidance note provides instructions on how to submit a Data Protection Impact Assessment and when to do so.

13. REGISTRATION WITH THE ODPC

Entities that process children's data are required to register as either data controllers or data processors. This applies to any organisation handling personal data related to children, ensuring compliance with the Act and safeguarding children's privacy and rights during data processing.

The Office has published a Guidance Note on Registration of Data Controllers and Data Processors which is accessible through www.odpc.go.ke The guidance note includes a step-by-step guide on how to complete the registration process and the information required during the registration process.

14. PROTECTION OF CHILDREN'S DATA ONLINE (SOCIAL MEDIA)

With the advancement of technology, the world is increasingly digitising, making the protection of personal data a crucial concern. Social media networks collect, store and share personal information, including sensitive data, underscoring the urgent need for robust measures to be taken to safeguard individual privacy.

Children form part of online consumers. Online access for children comes with different risks, including consuming age-inappropriate content, cyberbullying and even online predators who may take advantage of the child to share personal information, such as name, phone number, home address and school address. Due to these vulnerabilities that children face in the digital space, safeguarding their privacy is of extreme importance.

The Act requires any processing of children's data, even by social media platform owners, to be done lawfully. Parental or guardian consent should be mandatory for account creation. These platforms should implement robust age verification measures to confirm the age of users and obtain parental consent when required.

Social media platforms can implement measures to ensure the protection of children's data online, including but not limited to the following:

(i) Conducting a DPIA prior to the processing of children's data to ascertain the risk.
(ii) Platforms should design their systems with privacy protection embedded from the start, ensuring that only the minimum data necessary for the service is collected.
(iii) Having clear policies that inform the parents/guardians how personal data will be used, stored and shared.
(iv) Develop age-appropriate privacy settings. Platforms should apply the highest level of privacy for children's accounts, such as private profiles that limit who can view their content, limited data sharing and allow users to easily adjust privacy settings.
(v) Limit data collection so that only the necessary data is collected from children and the collection of sensitive data is avoided.
(vi) Implement appropriate technical and organisational measures to protect children's data, such as data encryption and/or anonymisation and pseudonymisation that ensures that any data that can directly identify a child is masked to protect their identity.
(vii) Develop data retention policies that define how long a child's data can be stored and ensure the data is automatically deleted or anonymised after a defined retention period.
(viii) Ensure algorithms for content curation or advertising prioritise children's best interests, avoiding exposure to inappropriate or manipulative content.
(ix) Conduct awareness campaigns to educate parents and children about online privacy, safe internet usage and the consequences of sharing personal data.

Parents and guardians have a role in ensuring the safety of their children's personal information online. To ensure the privacy and safety of personal information relating to children in the online space, measures that can be adopted include but are not limited to the following:

(i) Ensuring the child's account sets the required age during account setup.
(ii) Use the built-in parental controls or family safety centres, which offer additional security features and advice to manage children's platform usage.

(iii) Customising the privacy settings by adjusting settings to restrict who can view their child's profile, send messages or comment on posts.

(iv) On the respective social media platform, enable features that block or filter inappropriate or harmful content.

(v) Monitoring children's online activity and teaching them how to report and block harmful, inappropriate content or unwanted interactions.

(vi) Regularly discuss with the child the importance of privacy, data security, and prudent online behaviour and encourage them to be mindful about sharing personal information, such as their name, age, and location, that predators may use to cause harm.

Example:

SunguraApp is a social media app that is designed specifically for children. This social media platform prioritizes safe interactions and encourages creative expression, allowing kids to share their experiences in a fun and secure environment. As children create their profiles, they provide essential personal data like their name, age, and even a profile picture—often a playful avatar rather than a real photo. Through SunguraApp, they can share their photos and videos, showcase their creativity and connect with friends. The app also tracks interactions, such as messages sent, friendships formed, and likes on posts, all while ensuring that these connections remain safe.

Understanding the unique needs of its young users, SunguraApp places a strong emphasis on parental involvement. Before children can access the app, parents or guardians must give explicit consent, fully aware of the data being collected. They have the power to manage privacy settings, controlling who can see their child's content and interact with them. Data security is a top priority for SunguraApp. Every piece of information is encrypted and stored securely, ensuring that kids can enjoy their online experience without fear. Additionally, user accounts come equipped with privacy settings that limit public visibility, keeping interactions confined to a safe space.

The app maintains a responsible approach to data retention. Information is kept only as long as the account is active, and parents have the option to request the deletion of their child's account and all associated data whenever they choose. To foster a sense of transparency, SunguraApp provides regular updates to parents about their child's activities and data usage. This open line of communication helps build trust, ensuring that families can navigate the digital world together. In this way, SunguraApp not only offers a platform for children to connect and express themselves but also champions safety and responsibility, setting a new standard for social media in the lives of young users.

15. PENALTIES FOR NON-COMPLIANCE

Non-compliance with the Act's requirements for processing children's data can lead to significant penalties, including fines, reputational damage, and legal liability for social media platforms. The Office can impose fines and take other corrective measures where a platform fails to protect children's data adequately.

17. COMPLIANCE CHECKLIST:

	Processing children's personal data	**YES**	**NO**
1.	**Lawful Basis for Processing.**		
1.1	Have you identified a lawful basis for processing children's data?	[ ]	[ ]
2.	**Parental or Guardian Consent and Age Verification.**		
2.1	Have you obtained explicit parental/guardian consent where required?	[ ]	[ ]
2.2	Is consent informed and verifiable?	[ ]	[ ]
2.3	Have you implemented an age verification process?	[ ]	[ ]
3.	**Sensitive Data.**		
3.1	Have you determined whether the data qualifies as sensitive personal data, such as health or biometric information?	[ ]	[ ]
3.2	Have you obtained explicit consent or identified a lawful basis for processing sensitive data?	[ ]	[ ]
3.3	Have you implemented security measures for sensitive data (e.g., encryption)?	[ ]	[ ]
4.	**Purpose and Data Minimization.**		
4.1	Is the data collected only for specified, legitimate purposes?	[ ]	[ ]
4.2	Is the data collection limited to only what is necessary (data minimization)?	[ ]	[ ]
5.	**Data Accuracy and Retention.**		
5.1	Are you ensuring data accuracy and regular updates?	[ ]	[ ]
5.2	Have you defined clear retention periods for children's data?	[ ]	[ ]
6.	**Data Subject Rights.**		
6.1	Have you informed children or parents of their data subject rights?	[ ]	[ ]
6.2	Do you have a process for handling access requests?	[ ]	[ ]
6.3	Have you provided an option for parents to object or withdraw their consent?	[ ]	[ ]
7	**Security Measures.**		
7.1	Have you implemented technical security measures (e.g., firewalls, encryption)?	[ ]	[ ]
7.2	Have you implemented organisational security measures, e.g., staff training?	[ ]	[ ]

7.3	Is data access limited to authorized personnel only?	[ ]	[ ]
7.4	Have you designed systems with privacy protections by default?	[ ]	[ ]
8.	**Transparency.**		
8.1	Have you provided child-friendly and transparent privacy notices?	[ ]	[ ]
9	**Data Processors.**		
9.1	Have you vetted data processors to ensure compliance with data protection laws?	[ ]	[ ]
9.2	Have you established contracts with data processors specifying their obligations?	[ ]	[ ]
9.3	Do you conduct regular audits and monitoring data processors?	[ ]	[ ]
10.	**Data Protection Impact Assessment (DPIA).**		
10.1	Have you performed a Data Protection Impact Assessment (DPIA) for high-risk processing?	[ ]	[ ]
10.2	Have you implemented mitigation measures identified in the DPIA?	[ ]	[ ]
11.	**Breach Notification and Response.**		
11.1	Do you have a breach response plan in place?	[ ]	[ ]
11.2	Will you notify the ODPC within 72 hours in case of a data breach?	[ ]	[ ]
11.3	Will you notify parents in case of a breach involving children's data?	[ ]	[ ]
12.	**Compliance with the Office of the Data Protection Commissioner (ODPC)**		
12.1	Are you registered with the ODPC?	[ ]	[ ]
12.2	Do you have procedures in place for ongoing compliance and internal audits?	[ ]	[ ]