OFFICE OF THE DATA PROTECTION COMMISSIONER

GUIDANCE NOTE FOR THE EDUCATION SECTOR

DECEMBER 2023

TABLE OF CONTENTS

DEFINITIONS:

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

"Content data" means information contained in an electronic communication and which may include any attachment to such communication that attract a duty of confidentiality information relates to identifiable user of the service.

"Data" means information which -

a) is processed by means of equipment operating automatically in response to instructions given for that purpose;
b) is recorded with intention that it should be processed by means of such equipment.
c) is recorded as part of a relevant filing system.
d) where it does not fall under paragraphs (a) (b) or (c), forms part of an accessible record; or
e) is recorded information which is held by a public entity and does not fall within any of paragraphs (a) to (d).

"Data Commissioner" means the person appointed pursuant to section 6 of the Act.

"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 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.

"Entity" or **"Entities"** means a natural (individual) or legal person, public authority, agency or other body that processes (handles) Personal Data.

"Office" means the Office of the Data Protection Commissioner as established in section 5 of the Act.

"Personal Data" means any information relating to an identified or identifiable natural person.

"Privacy framework" is a set of guidelines, principles, and standards that organisations can use to protect the personal information of individuals.

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

"Protected System" means a computer system used directly in connection with, or necessary for: -

a) the security, defence or international relations of Kenya.
b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law.
c) the provision of services directly related to communications infrastructure, banking and financial services, payment and settlement systems and instruments, public utilities or public transportation, including government services delivered electronically.
d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services.
e) the provision of national registration systems; or
f) such other systems as may be designated relating to the security, defence or international relations of Kenya, critical information, communications, business or transport infrastructure and protection of public safety and public services as may be designated by the Cabinet Secretary responsible for matters relating to information, communication and technology.

"Register of Data Controllers and Data Processors" means the list of registered entities maintained and published by the Office of the Data Protection Commissioner.

"Regulations" means the Data Protection (General) Regulations, 2021; the Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021; and the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.

"Sector Regulator" means the Communications Authority of Kenya established under the Kenya Information and Communications Act, 1998 and Central Bank of Kenya

"Sensitive Personal Data" means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the Data Subject.

Accountability - the responsibility of individuals, organizations, or institutions to be answerable for their actions and decisions, and to accept the consequences of those actions and decisions;

Accuracy - the responsibility of individuals, organisations, or institutions (whether public or private) to ensure that personal data processed by them is factually correct, up-to-date and relevant for the purpose for which it is being processed;

Data subject - means an identified or identifiable natural person who is the subject of personal data;

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 personal data;

Data processor - means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller;

Education institutions - institutions established to provide educational services to students;

Ministry of Education - a governmental ministry of Kenya, that is in charge of national policies and programs that enable Kenyans t o gain access to high-quality, low-cost schoolinpost-secondaryary education, higher education, and academic research;

Office - means the office of the Data Protection Commissioner;

Personal data - means any information relating to an identified or identifiable natural person;

Sensitive personal data - means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject;

Stakeholders - a diverse group of individuals and organizations that contribute to the development and success of the education system.

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 Data Protection Act, 2019, which regulates the processing of personal data of persons located in Kenya by both private and public sector organizations.

The Office plays a vital role in ensuring that individuals have control over their personal data and that organizations 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 organizations 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, in particular, its digital superhighway initiative. As the digital landscape expands, the need for robust data protection mechanisms becomes paramount. The Office, with 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.

INTRODUCTION

The education sector is one of the largest users of personal data in Kenya, as it collects, stores, and analyzes vast amounts of personal data about students, teachers, and other stakeholders. From admission and enrollment data to academic performance, health information, and disciplinary records, educational institutions handle personal data that require careful handling to protect the privacy rights of involved individuals. This guidance note aims to provide education stakeholders with a comprehensive overview of their obligations when processing personal data and practical steps to ensure compliance with the law.

The Education Sector in Kenya is composed of sub-sectors, which include tarly Learning and Basic Education, Vocational and Technical Training, University Education and Research, Post Training and Skills Development, Implementation of Curriculum Reforms, and Regulators including the Ministry of Education with its state corporations, and the Teachers Service Commission, among others.

The education system provides services to over 16 million children and youth, with close to 500,000 teachers distributed across approximately 90,000 schools. The sector is increasingly expanding to accommodate more students, particularly in pre-school and post-primary education. Further, there are tens of universities and thousands of Public and private Technical and Vocational Education and Training (TVET) institutions.

These numbers highlight the vast amount and variety of personal data processed by the education sector and the number of individuals affected, including children. Notably, the National Education Management Information System (NEMIS) is one of the largest databases of personal data for Kenya's largest population.

Traditionally, the actors involved in processing the personal data of learners can be grouped into those who have a direct relationship with students, such as teachers and school administration, and those who do not, such as the Ministry of Education and its Semi-Autonomous Government Agencies (SAGAs) processing data for analytics purposes, examination, teacher performance, and progress measures.

However, the development of web-based data management solutions, and the use of new technologies in educational settings have significantly increased the number of commercial third-parties involved in processing students' data, including children's data.

This rise of Education Technologies (EdTech) and transition to offering education through digital applications has presented a range of challenges, particularly regarding privacy, with Edthe Tech industry being a frequent target of cyberattacksd data breaches, phishing and ransomware attacks, and account takeovers. These pose significant risks to eeducationalinstitutions and the data they collect and store.

This risk is often compounded by the lack of adequate data security measures and the involvement of parties in the education sector that may not follow the highest data protection standards. Additionally, hundreds of students using personal devices and connecting to institutional systems can further complicate data security concerns. Therefore, the framework of Data protection in the education sector in Kenya has become increasingly important. The right to privacy is enshrined in the Kenyan Constitution, as expounded under the Data Protection Act,

2019, which provides the required legal framework to all individuals and organizations that process personal data, including educational institutions.

PRIVACY CONCERNS

The nature of processing data in the education sector raises significant privacy concerns, including the potential misuse of personal data, lack of transparency around data collection and processing, and the risk of bias and discrimination in the processing of personal data.

A need has arisen for the education sector to take steps to ensure that personal data is collected and processed fairly and transparently, with appropriate data protection measures in place to safeguard personal data against unauthorized access, disclosure, or loss.

The use of digital technologies in education has compounded new challenges for data protection in Kenya. For example, educational institutions may collect and process personal data through online learning platforms, student information systems, and other digital tools. This data can be vulnerable to cyber-attacks and other security threats, which can result in data breaches and other privacy violations. The adoption of EdTech in the education sector has grown significantly in recent years, from basic to advanced levels. However, this transition to digital applications has come with its own set of privacy concerns. EdTech is increasingly becoming a target for cyberattacks, putting the privacy of collected and stored data at risk.

Frequent data breaches, phishing, and ransomware attacks are common, often caused by a lack of adequate data security measures and the involvement of EdTech parties that may not follow high data protection standards. Additionally, the risk of breaches arises with hundreds of students using personal devices and connecting to the institution's server.

Another critical privacy concern is how vendors use the personal data to which they have access. Untrustworthy vendors can collect and reuse personal data in ways that educational institutions, SAGAs, data subjects, and their legal guardians may be unaware of, such as using data for advertising purposes or packaging and selling data to third parties. The use of data for profiling and predictive analysis can have serious long-term effects, especially on children, and raises significant privacy concerns.

Cloud-based solutions present their own set of risks, such as non-efficient encryption algorithms or inherent security risks when all assets are hosted online. The most significant issue with cloud-based solutions is the minimal control over data and cloud system setup. The terms and conditions are determined by cloud service providers, and educational institutions as data controllers have very little power.

Surveillance technology is often accepted by parents and teachers as a safety instrument, but the pervasive use of student surveillance technology (including CCTV and tools to track students' online behaviour) can result in serious harm.

In addition to tech-related matters, there are other privacy concerns, such as displaying examination results of pupils/students on school notice boards, disproportionate data disclosures of academic records, financial obligations, behavioural issues, or sensitive data (including health data) to larger groups via students' or parents' WhatsApp groups or during parent-teacher meetings, publishing photos of top performers of exam results on the newspapers, among others.

Allowing parents unauthorized access to university students' records who are already adults by their parents paying the tuition fees, posting/using photos or video in the school prospectus and on the website without valid consent, accuracy of exam results and other data, collection and retention of excessive data or data for an extended period than necessary, and use of CCTV cameras in boarding schools poses high privacy concerns.

These privacy concerns can lead to infringement of the right to privacy and potentially result in bullying, discrimination, and exclusion. Educational institutions must understand that students and children do not lose their human rights by passing through the school gates, and education must be provided in a way that respects their inherent dignity and right to privacy. While the above list of challenges is illustrative, it is not exhaustive, and the education sector must remain vigilant and proactive in addressing privacy concerns.

SCOPE AND PURPOSE

The scope of this guidance note is to provide educational institutions with a clear understanding of their obligations under data protection law. The guidance note aims to cover various aspects of data protection, including the collection, use, retention, disclosure, and disposal of personal data in the education sector. The note will apply to all educational institutions operating in Kenya, including kindergartens, primary and secondary schools, and higher education institutions.

Further, the scope note extends to remote e-learning solutions and services to ensure that distance learning tools and resources comply with the same rigorous data protection standards as traditional in-person education. It will also cover any remote e-learning solutions and services that educational institutions engage in and use. It will emphasize the importance of due diligence in selecting and using distance learning tools and resources that meet data protection standards.

The note may include separate sections tailored to different educational institutions, such as primary schools, secondary schools, and higher education institutions and consider the specific data protection challenges and issues relevant to each type of institution. It will provide clear and practical guidance on various data protection principles, including the legitimacy and lawful basis for processing personal data, fair processing, data retention, security, automated decision-making, profiling, and the use of biometric data.

Lastly, it will include checklists to help school administrations understand the requirements and check their compliance with relevant legal requirements, including guidance on the creation of privacy notices, which must stipulate the rights of data subjects and how they can be exercised. Each school will be required to create an individual privacy notice covering the processing activities specific to their school. While certain sections of this guidance note may be applicable, compliance audits conducted may be necessary to provide tailored guidance and recommendations.

APPLICATION OF DATA PROTECTION PRINCIPLES

Data protection principles are crucial in the education sector to ensure that personal data about students and staff is appropriately collected, processed and stored. The principles ensure that individuals have control over their data and it is only used for the purposes for which it was collected.

LAWFULLY, FAIRLY AND A TRANSPARENT MANNER

Educational institutions are required to process personal data lawfully, fairly, and transparently. This means that they must have a valid legal basis for processing personal data and inform individuals of how the data will be used.

For instance, when collecting student data, institutions must obtain consent from the student or their parent/guardian and provide a clear explanation of why the data is being collected and how it will be used. To enhance transparency, educational institutions may create privacy notices that include:

- Categories and types of data processed
- The purpose(s) for which the information will be processed
- Information on how personal data will be collected
- Details on how data will be kept up-to-date
- Details on how confidential waste will be disposed of
- Information on what the school expects from staff who work with personal data
- Details on the use of security systems, such as computer passwords and firewalls
- Where necessary, how personal data is encrypted when held electronically
- Who is considered a trusted third-party
- Procedures for what to do if personal data is lost or stolen
- Rules for sharing or transferring data outside of the educational institution
- Rights of data subjects, including students, parents and staff
- Contact information, including contacts of the Data Protection Officer (where applicable)

The privacy notice should be included in any enrollment documentation and at the bottom of any forms used to collect personal information. It should also be easily accessible on the school's website where applicable. To emphasize transparency and build trust early on, institutions can also consider sending out a copy of the privacy notice to students and their parents at the start of each school year.

PURPOSE LIMITATION

The purpose limitation principle is a crucial aspect of data protection for educational institutions. This principle requires educational institutions to limit the collection and storage of personal data to only what is necessary for a specific purpose that has been communicated to the individual.

For instance, when collecting student data, educational institutions should only collect information that is relevant to the educational purposes for which it is being collected. This could include information such as academic records and attendance information. It is essential to communicate

the purpose of data collection to students and parents/guardians.

Example: A school may collect personal data from students and parents during the admission process, and must clearly state that the information will be used for admission purposes only, such as to provide necessary services, to communicate with the students and their family, or to manage student records.

Example: A school may collect information about a student's health for the purpose of providing necessary support in terms of medical cover, dietary needs and accommodations. The school cannot use this information for any other purpose without obtaining additional consent from the student or parents/guardian.

Example: Teachers Service Commission (TSC) must inform teachers that their information is collected for purposes of management of teachers in the country and not for sharing with banks for purposes of rendering financial services and offering loans.

DATA MINIMIZATION

Data minimization is a critical aspect of data protection for educational institutions. This principle requires institutions to limit the processing of personal data to only what is necessary for a specific purpose. This means collecting only the minimum amount of data required to achieve the educational purpose for which it is being collected.

For instance, when collecting student data, educational institutions should only collect information that is relevant to the educational purposes for which it is being collected. It is essential to communicate the purpose of data collection to students and parents/guardians to ensure that they understand what data is being collected and why.

To comply with the data minimization principle, educational institutions should regularly review the data they collect and determine if it is necessary for the intended purpose. This will help to ensure that data is not collected unnecessarily and that the institution is complying with data protection regulations. Educational institutions should also implement technical and organizational measures to ensure that personal data is not retained for longer than necessary.

Example: Education institutions should asks all job applicants to provide information about health conditions that are only relevant to particular occupations. It would be excessive to collect such information from all applicants and especially during the application phase.

ACCURACY

This principle requires that personal data should be current, consistent, complete and kept up to date. All institutions in the Education Sector must take reasonable steps to ensure that personal data is accurate and that any inaccuracies are corrected as soon as possible. Further, all institutions in the Education Sector must ensure that they make provision for internal controls to allow for verification of the information provided, allow for the updating of the personal data by data subjects and have regular periodic reviews. It is recommended that the reviews take place yearly.

Example: a school may keep a student's academic record and update it regularly with their grades and other relevant information. The responsibility lies with the school to ensure that this information is accurate and reflective of the students' actual performance.

Example: if a student's contact information changes, the educational institution must update their records to ensure that they can communicate with the student and their parents, for example, a school may ask for a student's email address for the purpose of sending them updates on school activities and assignments.

STORAGE LIMITATION

This principle requires that personal data should not be kept for longer than is necessary for the purposes for which it is processed in accordance with subsisting government policy and legislation. All institutions in the education sector must have appropriate internal policies and procedures in place to ensure that personal data is securely stored and only kept for as long as necessary. The said internal policies should hava e specified retention period in accordance with the laws governing the relevant educational institution or prevailing education policy or otherwise provide for reasonable and justifiable retention periods based on the processing activity and the identified purpose for processing.

Example: student records should be securely stored for a certain period of time after the student has left the educational institution, after which they should be securely destroyed and in compliance with relevant laws on destruction of records.

CONFIDENTIALITY AND INTEGRITY

This principle requires that personal data must be processed in a manner that ensures its security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

Example: a school may store the student records in a secure location and limit access to authorized personnel only. The school should also have appropriate technical and organizational measures in place to protect personal data from unauthorized access, loss or theft, and back-up the data regularly to prevent loss. Schools can also implement password protected systems to secure records among others.

ACCOUNTABILITY

This principle requires that all education institutions are responsible for complying with data protection principles (the Act and the Regulations). All institutions in the education sector must have appropriate policies and procedures in place to ensure compliance with data protection laws and must be able to demonstrate compliance.

Example: To demonstrate compliance with the data protection principles, educational institutions may adopt and implement data protection policies and 'data protection by design and default' approaches; maintain documentation of processing activities; implement appropriate security measures and appoint a data protection officer who is responsible for ensuring compliance with data protection laws and must conduct regular audits and risk assessments.

RELEVANT LAWFUL BASES FOR EDUCATIONAL INSTITUTIONS

The Act provides for eight lawful bases for processing personal data. Section 30 of the Act requires that personal data shall only be processed if at least one of the eight legal grounds listed in that Section apply. In particular, personal data shall only be processed if a data subject consents or the processing is necessary for:

- Performance of a contract
- Compliance with any legal obligation
- Protection of vital interests of the data subject
- Public interests
- Performance of a task undertaken by public authority
- Legitimate interests pursued by the data controller or processor
- Historical, statistical, journalistic, literature and art or scientific research.

CONSENT

In the context of the education sector, consent can only be an appropriate lawful basis if the data subject is offered a genuine choice concerning accepting or declining the terms offered or declining them without detriment. Minors cannot validly give consent, and such consent must be provided by their parent or legal guardian. Educational institutions must therefore ensure that they obtain valid consent and that the consent is specific, informed, and freely given. Section 2 of the Act defines the meaning of consent as being:

i. **Specific**: The data subject must be informed about the specific purpose for which their data will be processed.

> **Example:** If an educational institution wants to process a student's personal data for the purpose of conducting a research study, the student must be informed of this specific purpose for which personal data is provided for.

ii. **Informed**: The data subject must be provided with sufficient information to make an informed decision about whether or not to give consent. This includes information about the types of personal data that will be processed, how the data will be used, who will have access to the data, and how long the data will be retained.

iii. **Freely given**: The data subject must be given a genuine choice about whether to give consent or not. Consent cannot be coerced or forced, and there must be no negative consequences for the data subject if they refuse to give consent.

> **Example:** there is a number of unions in education sector. If a teacher does not want to join a certain union, he/she should not be forced to join the same.

For further information see the Office's Guidance Note on Consent available on www.odpc.go.ke

PERFORMANCE OF A CONTRACT

In the context of the education sector, contractual necessity may arise in several situations, such as:

i. **Admission and enrollment**: educational institutions may need to process personal data, such as academic records and contact details during admission.
ii. **Provision of educational services**: educational institutions may need to process personal data, such as attendance records and academic performance, to provide educational services to their students.
iii. **Employment contracts**: educational institutions may need to process personal data, such as employee contracts and payroll information, in relation to their employees.

Processing of personal data must be directly related to the performance of the contract and must be necessary for the parties to fulffulfilir obligations under the contract.

LEGAL OBLIGATION

To rely on legal obligation as a lawful basis for processing personal data, educational institutions must demonstrate that the processing is necessary for compliance with a legal obligation to which they are subject. This means that the processing must be directly related to the legal obligation and it must be provided in the legislation.

Legal obligations may arise from various sources, such as:

i. **Statutory and Regulatory requirements**: Maintenance of academic records and reports such as academic transcripts and attendance records are legal requirements.

> **Example:** In the Kenya School of Law Act No. 26 of 2012, the director is required to keep records of attendance of the students and the record is considered conclusive evidence of attendance of the students.

> **Example:** In the HELB Act No. 213A of 2012, it is a requirement that for HELB to offer any grant to an applicant they must fill the relevant prescribed form which requires personal details . They are then issued with a unique personal identification number.

ii. **Contractual obligations**: During the process of employing teachers, the TSC should obtain the personal details of the teachers as a preliminary requirement for the formation of any legally binding employment contract.

iii. **Statutory Obligations** such as NSSF, KRA or NHIF, are placed on employers with respect to deductiaboutg to their employees.

PUBLIC INTEREST

Public interest can be a lawful basis for the processing of personal data in the education sector if the processing is necessary for the performance of a task carried out in the public interest in the exercise of official authority vested in the educational institution. Public interest may arise from various sources, such as:

i. **Government mandates**: Education institutions may be required by the government to collect and report data related to their students and staff for statistical purposes, policy-making, and public accountability.
ii. **Public safety**: Education institutions may need to process personal data to ensure the safety and security of their students and staff, such as through the use of CCTV cameras and background checks.

PUBLIC TASK/AUTHORITY

Statement on Data Protection Considerations:

In the Kenyan education sector, public institutions, such as public schools and universities, may process personal data when carrying out tasks in the public interest or when exercising their official authority. This could include tasks related to the provision of education, administration, research, and other related activities. However, such processing must adhere to the principles of data protection and ensure that appropriate safeguards are in place.

Example:

The Ministry of Education in Kenya launches a nationwide program to track the academic progress of students in public schools to improve the quality of education. As part of this initiative, public schools are required to submit detailed academic records of students, including their names, identification numbers, and examination scores, to a centralized database managed by the Ministry.

Do's:

- The Ministry ensures that the data collection is strictly for the purpose of improving the education system and is carried out in the public interest.
- Schools inform parents and guardians about the data collection initiative, explaining its purpose and the safeguards in place.
- The Ministry implements robust data protection measures, such as encryption and restricted access, to protect the students' data in the centralized database.

Don'ts

- Schools should not share any additional personal data of students that is not relevant to the initiative.
- The Ministry should not use the data for any other purpose than what was specified.
- The data should not be shared with third parties or external organizations without a valid reason and without ensuring that adequate data protection measures are in place.

In this scenario, the processing of students' personal data by public schools and the Ministry of Education is justified on the basis of a public task or the exercise of official authority. However, it's crucial that the principles of data protection are upheld, and appropriate safeguards are implemented to protect the rights and interests of the data subjects.

LEGITIMATE INTERESTS

Legitimate interest can be a lawful basis for processing personal information in the education sector if the processing is necessary for the legitimate interests pursued by the educational institution or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject. This means that the educational institution must have a genuine and legitimate interest in the processing and that the data subject's rights and freedoms are not disproportionately affected by the processing. Legitimate interests may arise in various situations, such as:

i. **Fundraising**: Education institutions may process the personal data of students, alumni, and other stakeholders for the legitimate interest of promoting their programs, fundraising, and building relationships.
ii. **Research**: Educational institutions may process personal data for the legitimate interest of conducting research that contributes to the advancement of knowledge and academic excellence.
iii. **Security**: Educational institutions may process personal data for the legitimate interest of ensuring the security and safety of their premises, staff, and students.

HISTORICAL, STATISTICAL, JOURNALISTIC, LITERATURE AND ART OR SCIENTIFIC RESEARCH

Historical, statistical, journalistic, literature and art or scientific research may be conducted by educational institutions for various purposes, such as:

i. Educational research: Education institutions may process personal data for research purposes to improve the quality of education and contribute to the advancement of knowledge.
ii. Historical research: Education institutions may process personal data for historical research purposes to document and preserve the history of the institution and its community.
iii. Scientific research: Education institutions may process personal data for scientific research purposes to study human behavior behaviour topics.

> **Example:** During the Covid-19 period, Kenyatta University students with the help of their lecturers were at the forefront in coming up with ventilators as there was insufficient supply of the same.

iv. Statistical research: This is mostly possible through the quantitative research projects conducted by tertiary institution students as a requirement for the award of their degree.

To rely on historical, statistical, journalistic, literature and art or scientific research as a lawful basis for processing personal data, education institutions must ensure that the further processing for historical, statistical and/or journalistic purppurposesnot inconsistent with the original purpose of collection and the identified research purpose. This means that the use of the data for historical, statistical and research must be a secondary lawful purpose and should be directly related to the

initial purpose of collection or processing of the personal data and must be processed in a manner that would not result in the personal data being published in idean ntifiable format.

RIGHTS OF A DATA SUBJECT

Section 26 of the Data Protection Act affords several rights to a data subject. These are:

RIGHT TO BE INFORMED AND DUTY TO NOTIFY

The right to be informed means that data subjects have the right to be provided with clear and concise information about how their personal data will be used. It is an essential aspect of data protection law, which requires data controllers (i.e., education institutions) to provide individuals (i.e., students, teachers, and other staff members) with specific information about the processing of their personal data. This includes who will be processing the data, why it is being processed, and how long it will be retained.

Education institutions must provide individuals with information about the purpose and legal basis of the processing. This means explaining why the institution is collecting and processing personal data, and what legal basis it relies on (such as consent, legitimate interests, or legal obligation).

To comply with the right to be informed, schools should provide a privacy notice to data subjects. This notice should be easy to understand and accessible to all relevant individuals. When collecting personal data from students during enrollment, schools should provide a privacy notice that explains how their data will be processed, who will have access to it, and the purposes for which it will be used. Similarly, when collecting personal data from parents or guardians, schools should provide a privacy notice that explains how their child's data will be processed and why it is necessary.

Example 1: A primary school in Kenya collects personal data from pupils and parents during enrollment, including names, addresses, dates of birth, and contact information. To comply with the right to be informed, the school provides a privacy notice to all relevant individuals that explains how their personal data will be used, who will have access to it, and how long it will be retained.

Example 2: A university in Mombasa collects personal data from its students to process their applications for student loans. The institution provides students with a privacy notice that explains the purpose of the processing (to process student loan applications) and the legal basis (legal obligation under the Higher Education Loans Board Act).

> **Example:** A technical college in Nakuru shares personal data of its students with the Ministry of Education, the National Industrial Training Authority, and its service providers. The institution provides students with a privacy notice that lists the recipients of their personal data.

Education institutions must provide individuals with information about the recipients of their personal data. This means explaining who the institution shares personal data with, such as other educational institutions, government bodies, or service providers.

Education institutions must provide individuals with information about the data retention period. This means explaining how long the institution will retain personal data, or how this will be determined.

> **Example:** A primary school in Machakos retains personal data of its pupils for five years after they leave the school. The institution provides parents with a privacy notice that explains the data retention period and the reasons for it.

The duty to notify means that data controllers must inform the relevant authorities and data subjects in the event of a data breach. This duty is crucial for ensuring that data subjects take appropriate steps to protect themselves from potential harm.

To comply with the duty to notify, schools should have a clear procedure in place for reporting data breaches. This should include a designated person or team responsible for handling data breaches and notifying the relevant authorities and data subjects. Schools should also keep a record of all data breaches and how they were resolved.

> **Example 1:** A university in Kenya experiences a data breach that results in the unauthorized access of student data, including names, dates of birth, and academic records. To comply with the duty to notify, the university promptly reports the breach to the relevant authorities and notifies all affected students of the breach and the steps they can take to protect themselves from potential harm.

> **Example 2:** An education institution that discovers a data breach, such as the loss of a USB drive containing personal data of students, must notify the affected individuals and relevant authorities, such as the Office of the Data Protection Commissioner, within 72 hours of becoming aware of the breach. The notification should include information about the measures taken to recover the lost data and prevent future breaches.

RIGHT TO ACCESS PERSONAL DATA

All stakeholders have the right to access their personal data. This implies that students, parents and guardians have the right to request access to their personal data such as disciplinary records, health information and academic records. In relation to a child, a person with parental authority or guardian has the right to access any personal data held by the school. In accordance with the regulations, an institution in the education sector has seven (7) days following the receipt of a data access request within which to provide access to the information to the said data subject.

To exercise this right, individuals must make a written request to the institution in the education sector that holds that personal data. The institution must respond by giving access to the data, as this right is absolute.

> **Example:** For the Higher Education Loans Board that issues loans to individuals pursuing higher learning, all students that subscribe to the programme have the right to request access to their personal information. This access should be granted upon request through the HELB portal or visiting the HELB offices to peruse the records.

RIGHT TO OBJECT TO PROCESSING OF PERSONAL DATA

Section 26 of the Act provides for the "right to object". This means that a data subject or the guardian of a data subject can object to the processing of the data subject's personal data. Generally, schools must have written permission from the parent or eligible student itorelease any information from a student's education record. Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honours and awards, and dates of attendance.

However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school does not disclose directory information about them.

RIGHT NOT TO BE SUBJECT TO AUTOMATED DECISION-MAKING

Automated decision-making takes place when an electronic system uses personal information to make decisions without human intervention. If the personal information is digitally generated, the school should have safeguards for the protection of the information against digital manipulation. Automated processing is used for various purposes such as admission processes, student evaluations, and predictive analytics. However, the use of such systems may have a significant impact on the rights and freedoms of students, especially if the decisions are made without human intervention or oversight.

The right not to be subjected to automated decision-making in the education sector enables students and other stakeholders to challenge decisions made by automated systems, such as admission decisions or academic assessments. This right ensures that decisions that have a significant impact on students are reviewed by humans who can consider individual

circumstances, biases, and context.

However, it is important to note that the right not to be subjected to automated decision-making is subject to certain conditions and exceptions. For example, this right may not apply if the decision is necessary for the performance of a contract between the student and the education institution, or if the decision is authorized by law.

> **Example:** The National Education Management Information System portal provides an avenue for auto placement of student into a high school. Learners are issued with a Unique Personal Identifier immediately after being signed into the system. In the signing in process, the system uses the learner's birth certificate which contains personal data in relation to them. The NEMIS system in this case will fall under the exception to the right not to be subjected to automated decision making since it is crucial for a learner to have the NEMIS Unique Personal Identifier to ensure the performance of a legal obligation by the institution.

RIGHT TO RECTIFICATION OR ERASURE OF PERSONAL DATA

The right to rectification allows individuals to request the correction of their personal data that is inaccurate, obsolete, incomplete, false or misleading. This means that, if a student's personal information in the education system is incorrect, they have the right to request that it be updated or corrected. This is particularly important in the education system, where accurate records are essential for student progress and evaluation.

> **Example:** If the name in the KCPE, KCSE or Undergraduate certificate is misspelled, the holder of the certificate has the right to request the relevant education institutions for rectification of the names to reflect the right names.

The right to erasure commonly referred to as the right to be forgotten, on the other hand, allows education stakeholders to request that their personal data be deleted if there is no legitimate reason for it to be processed or if they have withdrawn their consent. This means that if a student or former student no longer wants their personal information to be stored or processed by the education system, they have the right to request its deletion.

> **Example:** A former student or alumni of a university in exercising their right to privacy, may request for the erasure of personal data from the institution's system, for example a photo of them that was being used for advertisement of the school.

RIGHT TO DATA PORTABILITY

The right to data portability is provided under Section 38 of the Act wherein a data subject may apply to port or copy their personal data from one data controller or data processor to another.

The right to data portability in the education sector thus allows data subjects to move, copy or transfer personal data easily without hindrance to usability enabling them to obtain and reuse their personal data held by the educational institutions across different services.

The right to data portability also ensures that educational institutions take necessary measures to make personal data available to the data subjects in a structured, commonly used, and machine-readable format.

However, the right to data portability is subject to certain conditions and exceptions. The right may not apply in the following circumstances:

a) where the processing may be necessary for the performance of a task carried out in the public interest or the exercise of an official authority;

b) it may adversely affect the rights and freedoms of others.

Additionally, the education institution may need to verify the identity of the requestor before providing access to the personal data to ensure the data is only disclosed to authorized individuals.

> **Example:** In the education sector, the right to data portability can be used by students or their parents/guardians to request and receive their personal data from an education institution, such as grades, transcripts, and other educational records. This right enables students to transfer their data to another education institution or to use it for other purposes, such as job applications or further education.

OBLIGATIONS OF EDUCATION INSTITUTIONS AS DATA CONTROLLERS AND/OR DATA PROCESSORS.

DUTY TO NOTIFY

One of the key principles of data protection is transparency. The personal data processed by an entity in the education sector shall be processed fairly and in a transparent manner. Therefore, at the time of collection, entities must comply with the obligations under Section 29 of the Act. This provision requires that data controllers and data processers notify data subjects of their rights specified in the Act; inform them that personal data is being collected, state the purpose of the collection; disdisclosey third parties who may receive the data and the safeguards adopted; provide the contacts of the data controller or data processor and disclose whether any other entity may receive the data; describe the technical and organizational security measures taken to ensure data confidentiality and integrity; state if the data is being collected pursuunderlaw and if it is voluntary or mandatory; and outline the consequences if data subjects fail to provide all or part of the requested data.

The above information should be provided to data subjects to enable them to understand how their personal data is used. The duty to notify should be contained in a data protection policy. The Data Protection Policy acts as a notice to individuals whose data is to be collected or otherwise processed. This policy must be brought to the attention of all individualsbeforeo the collection of their personal data or as soon as possible soon after where information is not collected directly. The data protection policy should also be provided to individuals upon request.

When drafting a Data Protection Policy, several practical considerations should be taken into account to ensure it effectively communicates to data subjects how their personal data will be used, these include:

a) the policy should be written in clear and plain language that is easy to understand. Technical or legal jargon should be avoided as much as possible to ensure that data subjects can easily comprehend what the policy says.
b) the policy should be transparent and comprehensive, covering all the relevant information that data subjects need to know about the processing of their personal data. This includes information about the rights of data subjects under the Data Protection Act, the fact that personal data is being collected, the purpose for which the personal data is being collected, the third parties to whom the data may be transferred, and any safeguards in place to protect the data.
c) the policy should be accessible to data subjects. This can be achieved by making it available on the data controller's or data processor's website, or by providing a copy upon request.
d) the policy should be reviewed and updated regularly to reflect any changes in data processing practices or relevant laws and regulations.

To make privacy policies easy for data subjects to understand, it is important to use plain language and avoid technical jargon. Visual aids such as infographics and diagrams can also be used to help convey complex information. In addition, using a question-and-answer format or breaking down the policy into shorter sections with clear headings can make it more digestible for data subjects. Providing examples of how personal data may be used in practice can also help

data subjects understand the policy and the implications of sharing their personal information.

Example: School X has digitized some of its enrolment processes and learning materials, and uses an online education platform that collects student information such as their name, email address, and billing information. In this case, the education platform could ffulfilits duty to notify by including clear language in its enrollment form or onboarding process about the types of data being collected and the purposes for which it is being used. The platform could also provide a link to its privacy policy and terms of service, which further explain the data processing and outline the rights of data subjects. Additionally, the platform could offer an opt-in mechanism for students, through their parents or guardians, to receive marketing materials.

To comply with the duty to notify, the school and app developer could provide clear language in the app's privacy policy that explains what types of data are being collected, the purposes for which it is being used, and the third parties (if any) that the data may be shared with. The privacy policy could also provide information on how parents or guardians can exercise their rights under data protection law, such as requesting access to their child's data or requesting that it be deleted.

In addition, the school could provide notice to parents or guardians at the time of enrollment or through a communication sent home, explaining that the app will be used in the classroom and what data will be collected. The school could also provide an opt-out mechanism for parents or guardians who do not wish to have their child's data collected or processed. Overall, it is important to provide clear and easily understandable information to parents and guardians so they can make informed decisions about their child's data privacy.

The data protection policy is an external facing document and is not to be confused with any internal policies that an entity develops to ensure internal practices align with the Data Protection Act. The common practice of demonstrating compliance with the laws and regulations among controllers and processors is through privacy policies and notices on websites. The information in a data privacy policy must be provided in simple and clear plain language, appropriate language for the target audience and be provided free of charge. The data privacy policy must be kept up to date to meet any changes in your approach to processing data.

PROCESSING OF SENSITIVE PERSONAL DATA IN THE EDUCATION SECTOR

The processing of sensitive personal data in the education sector is common, and education institutions must ensure that they comply with the law when processing such data because it requires a higher level of protection to safeguard the privacy rights of data subjects. It includes information about an individual's health, race, ethnicity, religion, biometric data, and sexual orientation, among others.

Generally, the processing of sensitive personal data is limited under the Data Protection Act, 2019 save for certain enumerated circumstances. To process sensitive personal data in the education sector, education institutions must meet certain conditions set out in data protection laws,

including obtaining explicit consent from data subjects, or ensuring that the processing is necessary for the performance of a legal obligation.

GUIDANCE:

a) Before collecting and processing sensitive personal data, education institutions should identify a lawful basis and purpose for the processing. Sensitive personal data should only be processed where there is a specific legal basis and a clear and legitimate purpose for the processing. For instance, schools can process the health data of students to safeguard their health and safety under the protection in the interest of the child basis.

> **Example:** A school may collect and process medical records of students to administer medication or provide necessary medical attention in case of an emergency.

b) Before processing sensitive personal data, educational institutions should obtain explicit consent from data subjects. This means that the data subject must give clear, unambiguous, and specific consent for their data to be processed.

> **Example 1:** A university may request explicit consent from students to process their biometric data for the purpose of accessing restricted areas within the institution.

> **Example 2:** A school may request explicit consent from a student or their parent/guardian to process their health information in cases where the student has a medical condition that requires special attention or treatment.

c) In certain circumstances, educational institutions may be required to process sensitive personal dattoto fulfillfulfillegal obligations. In such a case, the institution must ensure the procthating is necessary for the performance of a legal obligation. If personal data can be processed using less intrusive means, this should always be considered.

> **Example 1:** Schools may be required to collect information on the religious beliefs of students to facilitate the provision of religious education in compliance with legal requirements. In such cases, the processing of sensitive personal data must be necessary and proportionate to the legal obligation, and the data must be processed only for that specific purpose.

d) The processing is necessary to protect the vital interests of the data subject or another natural person or processing is necessary for the establishment, exercise, or defdefence legal claims:

> **Example 1:** A school may process a student's health information in an emergency situation where the student's life is at risk.

> **Example 2:** A university may process sensitive personal data related to a legal dispute with a former employee or student.

e) Where processing is permitted, educational institutions must take appropriate technical and organizational measures to ensure the security of sensitive personal data. For instance, a school nurse should have access to a student's medical records only if necessary for the provision of medical care, and the records should be kept confidential. This includes measures such as limiting access to the data, using encryption or pseudonymization and implementing access controls.

> **Example 1:** In exceptional cases, where no less intrusive methods can achieve the same aim, schools may use biometric data for access control to school premises, but must ensure that the biometric data is securely stored and accessed only by authorized personnel.

> **Example 2:** A primary school may implement access controls to ensure that only authorized staff can access sensitive personal data of pupils, such as medical records.

f) Educational institutions should only retain sensitive personal data for the period necessary to achieve the purpose of the processing. Sensitive personal data should be deleted or anonymized once it is no longer necessary for the processing.

g) In conclusion, processing sensitive personal data in the education sector requires careful consideration and adherence to data protection laws. Education institutions must ensure that sensitive personal data is processed lawfully, securely, and for a legitimate purpose. Failure to comply with data protection laws can result in significant fines, reputational damage, and legal liability. By following this guidance note, educational institutions can ensure compliance with data protection laws when processing sensitive personal data.

SHARING PERSONAL DATA TO PUBLIC AUTHORITY/AGENCY WHERE THERE IS A LEGAL OBLIGATION

When using legal obligation as a lawful basis for processing personal data, this includes the sharing of personal information, an entity must first demonstrate that the processing is necessary to comply with a legal obligation to which the entity, as the data controller, is subject. This can include obligations under national or country laws such as laws governing the provision of education, employment, or health and safety regulations.

Some of the considerations that must be considered when using legal obligation as a lawful basis for transferring personal data to a government agency or authority:

a) Identify the specific legal obligation that requires you to share personal data.
b) Ensure that the sharing is necessary to comply with that legal obligation. You must first clearly identify the legal or statutory requirement, and determine the scope of sharing and the personal data that is subject to the legal requirement.
c) Make sure that the personal data you share is relevant and limited to what is necessary to comply with the legal obligation. Therefore, only the information required to comply with the legal obligation should be extracted and shared.
d) Provide clear and transparent information to data subjects about the sharing, including the legal basis and the purpose. Information should be provided to parents, guardians, students over the age of maturity, teachers or any other data subject affected by way of a data protection policy notice (discussed above) before the sharing.
e) Ensure that you have appropriate security measures in place to protect the personal data you will transfer.
f) Retain personal data only for as long as necessary to fulfil the legal obligation.

Conversely, the Public Authority/ Agency receiving this information has a duty to ensure that data subjects acanexercise their rights. Further, the Public Authority/Agency must inform the individuals whose personal data they have received of why they are processing the information, their rights, and other information that should be included in a data protection policy, prior to the collection of their personal data or as soon as possible after they have received this data.

Example: University X is requested to transfer personal data of its students to HELB to enable remittance of student loans. This sharing of information is routine and the University is hesitant to share such information due to Data Protection Laws.

The University can rely on the provision on the HELB Act which creates a legal obligation. The University should also inform the students that such sharing is to be done in accordance with the HELB Act and provide details of the information that will be shared about students obtaining loans from HELB.

PRIVACY BY DEFAULT OR DESIGN

The Data Protection Act, in section 41, outlines the requirement for data controllers and data processors to implement appropriate technical and organizational measures to ensure effective implementation of data protection principles and necessary safeguards in data processing. Additionally, the Act requires that only necessary personal data is processed, taking into account the amount of data collected, the extent of its processing, storage period, accessibility, and cost of processing.

Data protection by design is an approach that ensures data controllers and data processors consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle. Data protection by default requires institutions in the education sector to ensure that only data that is necessary to achieve your specific purpose is processed. Data protection by default requires entities to ensure that data protection issues have already been considered and protection methods incorporated into existing systems and practices. This could be achieved by institutions in the education sector specifying the personal data required before the processing starts, appropriately informing individuals and only processing the personal data needed for the specific purpose.

Entities in the education sector are usually involved in processing student, parent, teacher data and other classes of data subjects that interact with these entities. Applying appropriate security measures to such data, and its processing environments both at rest and in transit, is vital to ensure the personal data is protected to the highest standards. Security measures should take into account the current state of the art data-security methods and techniques in the field of data processing.

EXAMPLE:

Entities in the education sector should take appropriate security measures to ensure against accidental or unauthorized access to, destruction, loss, use, modification or disclosure of personal data. These measures include: training in privacy and security; access controls; confidentiality agreements; and physical controls. In the education sector, appropriate measures could include implementing a robust student data management system with access controls, regular data backups, and encrypted data transmission channels.

For example, a school may adopt a cloud-based student management system with multi-factor authentication and strong encryption of data transmission to ensure that only necessary data is processed and safeguarded from unauthorized access or breaches.

In addition to the above, Data Protection Impact Assessment should be conducted prior to processing and should assess whether data is protected against unauthorized access, modification and removal/destruction. A Data Protection Impact Assessment should seek to achieve outcomes that embed high standards of security throughout the processing. Such an assessment must be informed by considerations of necessity and proportionality, and the fundamental data protection principles across the range of risks including physical accessibility, networked access to devices and data, and the backup and archiving of data.

Taking into account the nature and volume of the data processed and the risks for data subjects, including children, data security measures also refer to specific organizational measures such as:

- Physical security of paper files;
- Shredding all confidential waste;
- Keeping devices under lock and key when not in use;
- Not leaving papers and devices lying around;
- A written information security policy outlining the responsibilities of all staff members in protecting personal data;
- Regular training for all staff members on data protection best practices and the importance of maintaining the confidentiality of personal data;
- Regular internal and external audits to assess the effectiveness of technical and organizational safeguards.

Entities should ensure that they are continuously raising awareness on data protection amongst staff and their stakeholders. This should also include raising awareness internally of security measures that schools and tertiary institutions are implementing and the proper procedures for carrying out tasks related to personal data.

CHILD DATA PROTECTION CONSIDERATIONS

In addition to the above, entities in the education sector should take into account the following considerations:

PARENTAL CONSENT:

Parental/guardian consent is an important aspect of data protection, particularly when it comes to collecting and processing data about children. Parental/guardian consent is required before collecting or processing data about minors. Parental/guardian consent means that a parent or guardian has given permission for their child's data to be collected and used for specific purposes.

VERIFICATION OF AUTHORITY OF PARENTS OR GUARDIANS:

To ensure that parental consent is genuine, it is important to verify the authority of parents or guardians. Verification can be done in a variety of ways, such as by requiring a signed consent form, checking government-issued identification, or using electronic signatures. It is also important to ensure that the person giving consent is actually the child's parent or guardian, and not an imposter.

Example: An online learning platform asks parents to provide their child's full name and grade level, as well as a parent's email address, and then sends an email to the parent to confirm their identity and authority to consent.

AGE VERIFICATION:

Age verification is another important tool for protecting children's privacy online. Age verification helps to ensure that children do not access inappropriate content or services that could be harmful to them. Examples of age verification methods include requiring users to enter their date of birth, using identity documents, or conducting age checks with a third-party service.

CHILD CONTROLS:

Child controls are features that give teachers, parents or guardians the ability to control their child's online activities and protect their privacy. These controls can include setting limits on screen time, monitoring online activity, and blocking inappropriate content. Examples of child control features include parental controls on devices, content filtering options on social media platforms or EdTech applications.

Example: the learning management system provides a feature that allows teachers to monitor student activity and provide feedback, while also allowing parents to monitor their child's progress and activity within the platform.

Ensuring that parents or legal guardians have given their consent, verifying their authority, verifying age, and providing child controls are essential measures for protecting children's privacy. By incorporating these measures into their platforms and services, entities in the education sector can help to ensure that children's data is collected and processed in a responsible and transparent manner, and that their online experiences are safe and appropriate for their age.

PUBLISHING OF EXAM RESULTS:

Publishing children's examination results can be a sensitive issue. Examination results are personal data, and their unauthorized disclosure can lead to embarrassment, stigma, or other negative consequences for the child. It is crucial to handle such data with utmost confidentiality and ensure that it's shared only with authorized individuals.

The key principle is respecting the privacy rights of children and ensuring that their personal data is handled with care and responsibility. Institutions in the education sector must prioritize obtaining informed consent from parents or guardians before sharing any information related to children.

Example:

At the end of the term, Mr. Mutai, the school's principal, wants to celebrate the top-performing students by publishing their names and scores on the school's notice board and website.

Do's:

- Mr. Mutai sends out consent forms to parents, explaining the intention behind publishing the results and seeking their permission.
- He ensures that only the results of students with granted permissions are displayed.
- He provides an option for parents who are okay with the name being published but not the exact scores.

Don'ts:

- Mr. Mutai does not publish results without obtaining explicit consent from parents.
- He doesn't disclose any other personal information about the students, such as their addresses or class sections.

TAKING PHOTOS IN SCHOOL:

The publication of children's photos in the education sector raises significant data protection concerns. A child's image is considered personal data, and its unauthorized use or distribution can infringe on the child's right to privacy. It's essential to obtain explicit consent from parents or guardians before publishing or sharing any photographs of children, especially in public domains.

Example:

At the annual school sports day, Ms. Sulwe, the school's PR officer, wants to capture the day's events and share them on the school's website and newsletter.

Do's:

- Before the event, Ms. Sulwe sends out consent forms to all parents, explaining the purpose of the photos and where they will be published.
- She ensures that only children with granted permissions are photographed.
- She uses general shots (e.g., crowd scenes) where individual children are not easily identifiable.

Don'ts:

- Ms. Sulwe does not post photos with children's names or other identifying information.
- She does not use the photos for any other purpose than what was specified in the consent

ENGAGEMENT OF DATA PROCESSORS

Many educational institutions work with vendors/ service providers (data processors) providing different cloud-based, learning management systems and data management solutions, or security guard services. Education institutions should consider the vendors they engage and ensure that they opt only for a data processor who provides sufficient guarantees that processing will meet the requirements under the Act and protect data subjects' rights. In particular, in instances where data is processed by vendors or service providers, entities in the education sector must remain aware of their ongoing responsibilities as data controllers. Controllers must demonstrate due diligence to establish the vendor's/ service provider's ability to protect personal data.

To assist with this, the Act sets out that where an entity engages a vendor or service provider (processor) to process information on its behalf, there must be a written contract stipulating that the processor acts only on the controller's instructions and is bound by the obligations of the controller. Further, both parties should take all reasonable steps to ensure that any person employed by or acting under the authority of the data controller or data processor complies with the relevant security measures.

The Data Protection Act and related regulations specify that a contract between a data controller and data processor should include key elements, such as the subject matter of processing, the type of personal data, the nature and duration of processing, security measures, and situations requiring prior authorization from the controller. The contract must also outline the obligations of the processor to ensure staff confidentiality, assist the controller in meeting its obligations under the Act, and delete or return personal data at the end of the contract. The contract should include provisions for auditing and inspection, as well as liability in case of failure to meet obligations or acting outside the controller's instructions.

Example:

Data Controller (DC): A primary school that processes student and teacher personal data.

Data Processor (DP): An IT service provider that the DC has outsourced to manage its IT infrastructure and student information system.

Contract Terms: The contract between the DC and the DP includes the subject matter of processing, which is the management and processing of student and teacher personal data, including their names, addresses, dates of birth, and academic records. The contract specifies that the DP will ensure that its staff processing the data are subject to a duty of confidence, and appropriate measures to ensure the security of processing will be taken, including regular backups of data. The contract also stipulates that any personal data breach will be promptly reported to the DC. The DP is obliged to delete or return all student and teacher data to the DC at the end of the contract, and the DC has the right to audit and inspect the DP's data protection measures. The contract also outlines the liability of the DP if it fails to meet its obligations, including compensation for any damages caused to the DC or its students due to a breach.

DATA PROTECTION IMPACT ASSESSMENT

The carrying out of a DPIA is only mandatory where processing is "likely to result in a high risk to the rights and freedoms of data subjects". In cases where it is not clear whether a DPIA is required, it is recommended that a DPIA is carried out nonetheless as a DPIA is a useful tool to help data controllers and/or data processors comply with data protection law. In addition to the aforesaid, the Act requires that all data controllers and processors implement appropriate technical and organizational measures and integrate appropriate safeguards to ensure the adequate protection of 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 includes the form in which a Data Protection Impact Assessment should be submitted and guidance on when it should be submitted.

REGISTRATION WITH THE ODPC

Institutions in the education sector are expected to register as a data controller or data processor. Further, educational institutions are subject to mandatory registration regardless of their size and/or their annual turnover/ revenue.

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.

NOTIFICATION AND COMMUNICATION OF BREACH

Education institutions have to report personal data breaches to the ODPC without delay within 72 hours of becoming aware of the breach. Where there has been unauthorized access, schools, universities and other players within the education sector are required to communicate to the affected data subjects in writing within a reasonable period, unless the identity of the data subject cannot be established.

Entities are required to report data breaches to the Office and provide certain information about the breach. This information includes the date and circumstances in which the data breach was discovered, a chronological account of the steps taken after the breach was discovered, and details on how the breach occurred. Additionally, entities must provide the number of data subjects affected, the personal data or classes of personal data affected, and the potential harm to affected data subjects. The entity must also provide information on any action taken to mitigate the harm and remedy any failure or shortcoming that contributed to the breach, and how affected individuals can mitigate potential harm

> **Example:** A school collects personal data from students and staff members, including names, addresses, and academic records. The school's IT department discovers that an unauthorized person has gained access to the school's computer system, which contains sensitive personal data. The school immediately launches an investigation and determines that the breach is a notifiable data breach. The school promptly notifies the Office of the Data Protection Commissioner, providing a detailed account of the breach and the steps taken to mitigate harm. The school also informs affected individuals about the breach, advises them on how to eliminate or mitigate potential harm, and assures them that it will implement additional security measures to prevent future breaches.

The breach notification can be filed with the Office in a number of ways, including through a breach notification form accessible through www.odpc.go.ke, by email or by post.

ANNEX 1: CHECKLIST

	Question	Yes	No	Comments/ Remedial Action
Processing personal data based on consent	Have you reviewed your organisation's mechanisms for collecting consent to ensure that it is freely given, specific, informed and that it is a clear indication that an individual has chosen to agree to the processing of their data by way of a statement or a clear affirmative action?			
	Are procedures in place to demonstrate that an individual has consented to their data being processed?			
	Are procedures in place to allow an individual to withdraw their consent to the processing of their personal data?			
Processing children's personal data	Are procedures in place to verify the age of a child. Have you obtained consent from a parent/ legal guardian?			
Processing personal data based on legitimate interests	If legitimate interest is a legal basis on which personal data is processed, has an appropriate analysis been carried out to ensure that the use of this legal basis is appropriate? (That analysis must demonstrate that 1) there is a valid legitimate interest, 2) the data processing is strictly necessary in pursuit of the legitimate interest, and 3) the processing is not prejudicial to or overridden by the rights of the individual)			

DATA SUBJECTS RIGHTS

	Question	Yes	No	Comments/ Remedial Action
Access to personal data	Is there a documented policy/procedure for handling Data Subject Access Requests?			
	Is your organisation able to respond to Data Subject Access requests within seven days?			
Data portability	Are procedures in place to provide individuals with their personal data in a structured format, including a machine-readable format?			
Deletion and rectification	Are there controls and procedures in place to allow personal data to be deleted or rectified (where applicable)?			
Right to restriction of processing	Are there controls and procedures in place to halt the processing of personal data where an individual has on valid grounds sought the restriction of processing?			
Right to object to processing	Are individuals told about their right to object to certain types of processing such as direct marketing?			
	Are there controls and procedures in place to halt the processing of personal data where an individual has objected to the processing?			
Profiling and automated processing	If automated decision making, which has a legal or significant similar affect for an individual, is based on consent, has			

	explicit consent been collected?			
	Where an automated decision is made which is necessary for entering into, or performance of, a contract, or based on the explicit consent of an individual, are procedures in place to facilitate an individual's right to obtain human intervention and to contest the decision?			

ACCURACY AND RETENTION

	Question	Yes	No	Comments/ Remedial Action
Purpose Limitation	Are personal data only used for the purposes for which they were originally collected?			
Data minimisation	Are the personal data collected limited to what is necessary for the purposes for which they are processed?			
Accuracy	Are procedures in place to ensure personal data are kept up to date and accurate and where a correction is required, the necessary changes are made without delay?			
Retention	Are retention policies and procedures in place to ensure data are held for no longer than is necessary for the purposes for which they were collected?			
	Do you have procedures in place to ensure data are destroyed securely, in accordance with your retention policies?			

TRANSPARENCY REQUIREMENTS

	Question	Yes	No	Comments/ Remedial Action
Transparency to data subjects	Are individuals fully informed of how you use their data in a concise, transparent, intelligible and easily accessible form, using clear and plain language?			
	Where personal data are collected directly from the individuals, are procedures in place to ensure you have complied with your duty to notify?			
	Are procedures in place to ensure personal data are kept up to date and accurate and where a correction is required, the necessary changes are made without delay?			
	If personal data are not collected from the subject but from a third party (e.g. shared due to legal obligation) are procedures in place to provide a data protection policy to the individuals?			
	When engaging with individuals, such as when providing a service or CCTV monitoring, are procedures in place to proactively inform individuals of their data protection rights?			
	Is information on how the organisation facilitates individuals exercising their data protection rights published in an easily accessible and readable format?			

OTHER DATA CONTROLLER OBLIGATIONS

	Question	Yes	No	Comments/ Remedial Action
Data Processor Agreements	Have agreements with data processors (such as suppliers and other third parties) processing personal data on your behalf been reviewed to ensure all appropriate data protection requirements are included?			
Data Protection Impact Assessments (DPIAs)	If your data processing is considered high risk, do you have a process for identifying the need for, and conducting of, DPIAs? Are these procedures documented?			

DATA SECURITY

	Question	Yes	No	Comments/ Remedial Action
Appropriate technical and organisational security measures	Have you assessed the risks involved in processing personal data and put measures in place to mitigate against them?			
Documented security programme	Is there a documented process for resolving security related complaints and issues that specifies the technical, administrative and physical safeguards for personal data?			

	Is there a designated individual who is responsible for preventing and investigating security breaches?			
	Are industry standard encryption technologies employed for transferring, storing, and receiving individuals' sensitive personal information?			
	Are personal data systematically destroyed, erased, or anonymised when they are no longer legally required to be retained.			
	Can access to personal data be restored in a timely manner in the event of a physical or technical incident?			

DATA BREACHES

	Question	Yes	No	Comments/ Remedial Action
Data Breach Response Obligations	Does the organisation have a documented privacy and security incident response plan?			
	Are there procedures in place to notify the Office of the Data Protection Commissioner of a data breach?			
	Are there procedures in place to notify data subjects of a data breach?			
	Are plans and procedures regularly reviewed?			
	Are all data breaches fully documented?			
	Are there cooperation procedures in place between data controllers, data processors and other partners to deal with data breaches?			