WESTON
VIRTUAL SCHOOL
The pearl of Excellence and innovations

DATA PROTECTION POLICY

Reviewed by:	**Data Protection Officer**
Date of Policy:	September 2025
Review Frequency:	Annually
Review Date:	September 2026

1 Policy Statement

At Weston Virtual School, we are committed to ensuring the protection of personal data in accordance with the General Data Protection Regulation (GDPR) (EU Regulation 2016/679) and the Kenyan Data Protection Act, 2019 ("the Data Protection Laws"). As an online educational institution, we collect and process various types of personal data, including that of Students, staff, parents, guardians, and other stakeholders. This Data Protection Policy outlines the practices we follow to ensure that personal data is collected, processed, stored, and protected appropriately and in compliance with data protection laws.

2 Policy brief and purpose

The purpose of this Data Protection Policy is to demonstrate our commitment to maintaining high standards of privacy and protection of personal data in compliance with data protection laws and to demonstrate our commitment to handling the information of employees, Students, parents/guardians,stakeholders, and other interested parties with the utmost care and confidentiality.

This policy outlines how we process personal data in accordance with the principles and rights enshrined in both the GDPR and the Kenyan Data Protection Act, 2019, ensuring that:

- Personal data is processed lawfully, fairly, and transparently.
- Personal data is collected for specified, legitimate purposes and not further processed in a manner incompatible with those purposes.
- We minimise the data we collect and process and ensure it is accurate and up to date.
- We maintain robust security measures to protect personal data.
- We respect the rights of data principals and ensure that they can exercise those rights effectively.

This policy applies to all personal data collected and processed by the Institution, regardless of format, whether in electronic or paper form.

3 Scope

This policy applies to:

i). Students: Personal data collected from Student for enrolment, academic performance, health, and other purposes.

ii). Parents and Guardians: Data related to parent/guardian contact details, emergency contacts, and communication regarding Students.

iii). Staff: Personal and employment-related data such as contact information, qualifications, salary, and performance records.

iv). Third Parties: Data shared with third-party service providers or contractors who process personal data on behalf of the Institution.

It covers all forms of data processing, including collection, recording, storage, sharing, and deletion, across various departments within the Institution, such as academic, administrative, and student welfare services.

4 Definition of Data Protection Terms

i). Data – Information that is processed, stored, or used in a manner that relates to an identified or identifiable natural person. This includes both personal data and sensitive personal data.

ii). Data Subjects – An identified or identifiable person whose personal data is processed by the school (e.g., staff members, parents/guardians, and Students).

iii). Processing – Any activity that involves the use of personal data, including collecting, recording, storing, retrieving, disclosing, erasing, or destroying data.

iv). Personal Data – Any information that relates to an identified or identifiable natural person. Data that can directly or indirectly identify an individual (name, ID/Passport, Phone number, email Address, IP address).

v). Sensitive Personal Data – Data that refers to a special category of personal data that is considered more sensitive due to its nature reveals racial or ethnic origin, political opinions, religious beliefs, health data, genetics, or legal matters.

vi). Privacy Notices – These are clear and concise documents that we provide to individuals (data subjects) to explain what personal data we collect about them, why we collect it, and how we are legally allowed to do so. It is a way of being transparent about how we handle their information.

vii). Data Controllers – The data controller is the organization or entity (in this case, the School) responsible for deciding why and how personal data is processed. Essentially, we determine the purpose of collecting the data and how it will be managed throughout its lifecycle.

viii). Data Users – Data users are the staff members at the School who handle or process personal data as part of their job duties. These individuals are entrusted with access to personal information to perform their tasks while adhering to the principles of data protection.

ix). Data Protection Officer (DPO) – The person appointed as such under the Data Protection Act 2019 and GDPR. A DPO plays a critical role in ensuring data protection compliance, advising the schools, managing risks, serving as a liaison between the schools and the Office of the Data Protection Commissioner (ODPC).

x). Data Breach – A security incident that compromises the confidentiality, integrity, or availability of personal data. When such a breach occurs, the school is legally required to notify both the ODPC and the affected data subjects to mitigate any harm.

xi). **Privacy by Design and Default** – A principle requiring the integration of privacy protection into the design of systems and processes from the start and to ensure that by default only the minimum necessary personal data is collected, processed, and shared.

5 Policy components

Under the Data Protection Act 2019 of Kenya and the General Data Protection Regulation (GDPR) of the European Union, Weston Virtual School is committed to the responsible collection, processing, and management of personal data. These data protection laws are designed to protect the privacy and rights of individuals whose data we collect and process, ensuring that personal data is handled in a secure, transparent, and lawful manner.

Weston Virtual School adheres to the principles set out by both the Data Protection Act 2019 and the GDPR, which establish clear guidelines for data handling. These principles reflect our commitment to ensuring the privacy, confidentiality, and rights of all individuals whose personal data we process.

6 Data Protection Principles

In line with the GDPR and the Kenyan Data Protection Act, 2019, the Institution adheres to the following seven key principles when processing personal data:

i). Lawfulness, Fairness, and Transparency: Personal data must be processed lawfully, fairly, and in a transparent manner. Individuals will be informed about how their data is used, why it is needed, and how long it will be retained.

ii). Purpose Limitation: Personal data will be collected only for specified, legitimate purposes related to the educational activities of the Institution, such as student enrolment, academic performance monitoring, and regulatory compliance. Data will not be used for purposes incompatible with those for which it was initially collected.

iii). Data Minimisation: The Institution will ensure that only the personal data necessary for the specified purposes will be collected and processed. Unnecessary or excessive data will not be collected.

iv). Accuracy: Personal data will be kept accurate and up-to-date. The Institution will take all reasonable steps to ensure that data which is inaccurate or incomplete is rectified or deleted promptly.

v). Storage Limitation: Personal data will be retained only for as long as necessary to fulfil the purposes for which it was collected, or as required by law. Once the data is no longer needed, it will be securely deleted or anonymised.

vi). Integrity and Confidentiality: Personal data will be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, or destruction.

vii). Accountability: The Institution is responsible for ensuring compliance with these principles and will take steps to demonstrate adherence to data protection laws.

In addition, Weston Virtual School is committed to respecting the rights of data subjects as outlined in the Data Protection Act 2019 and GDPR. These rights include:

- **Right to be Informed:** As data subjects you will be informed about the data we collect, how it is used, and who has access to it.
- **Right of Access:** As a data subject you can request to see your personal data and understand how it is been processed.
- **Right to Rectification:** As a data subject you can request corrections if your data is inaccurate or incomplete.
- **Right to Erasure:** As a data subject you can request your data to be deleted in certain circumstances.
- **Right to Restrict Processing:** As a data subject you can request us to limit how your data is processed in specific situations.
- **Right to Data Portability:** As a data subject you can request the schools to for your data to be transferred to another service provider electronically.
- **Right to Object/consent withdrawal:** As a data subject you can object to certain types of data processing, such as for marketing purposes and withdraw your consent at any time by notifying the schools in writing.

7 Data Collection and Processing
Weston Virtual School will collect and process personal data for various legitimate educational, administrative, safeguarding and regulatory purposes, including but not limited to:

7.1 Pupil Data
i. Enrolment Information: Name, date of birth, contact details, guardianship details, previous academic history, and nationality.
i**i. Academic Records:** Performance data, grades, transcripts, attendance, and disciplinary records.
iii. Health Data: Medical conditions, vaccinations, allergies, disability status, and any accommodation or special needs.
i**v. Extracurricular Activities:** Participation in virtual clubs, online events, and other non-academic activities.

7.2 Staff Data
i. Personal Details: Name, address, date of birth, gender, and contact information.
i**i. Employment Information:** Employment contract details, job position, salary, qualifications, performance reviews, and payroll data.
iii. Health and Safety Information: Emergency contact information, medical records, and information related to any health accommodations.

7.3 Parent and Guardian Data
i. Contact Information: Parent or guardian names, addresses, phone numbers, and email addresses.
ii. Emergency Contacts: Individuals designated to be contacted in case of an emergency involving the student.

7.4 Third-Party Data
The Schools may also collect and process personal data on behalf of third parties (e.g., service providers, examination bodies, or government authorities), always ensuring that data protection contracts are in place to protect the data.

8 To exercise data protection, we are committed to implement some measures to ensure that data protection is enforced.
i). Train all the School employees on data protection requirements.
ii). Limit access to personal data to those who need it to perform their job duties.
iii). Securely store and protect data from cyber threats or unauthorized access.
iv). Implement clear procedures for reporting data breaches and ensuring compliance with data protection laws.
v). Establish secure practices such as shredding documents, regular backups, access authorization, and ensuring lockable desks and cupboards are used for physical records.

9 Use of Personal Information by the School.

With consent, the school will, make use of personal data relating to staff, Students, their parents/guardians, as follows. Any individual willing to withdraw consent should notify the school in writing.

i. **Images (photos or videos):** For school publications, website, and promotional materials.

i**i. Marketing:** To maintain contact with Students and parents for relevant communications.

10 Registration of Data Controllers and Processors

In accordance with the Data Protection Act, 2019 (Kenya), the schools, as a data controller, is registered with the Office of the Data Protection Commissioner (ODPC). All data processors working on behalf of the school are also required to comply with relevant data protection regulations.

11 Transfer of Personal Data Outside Kenya

Weston Virtual School will only transfer personal data to another country if:

- The recipient organization ensures adequate safeguards for the protection of personal data.
- The data subject has explicitly consented to the transfer.
- The transfer is necessary for the performance of a contract.

12 Providing Information over the Telephone

Staff members should be cautious when disclosing personal data over the phone. They must verify the identity of the caller and ensure that the information is only shared with authorized individuals. If the caller's identity cannot be confirmed, the request should be put in writing.

13 Accountability and Compliance

Weston Virtual School is committed to ensuring that personal data is processed in line with the GDPR and the Data Protection Act, 2019 (Kenya). This includes:

i. Appointing a qualified DPO to monitor compliance and provide advice.
ii. Implementing Privacy by Design and completing a Data Protection Impact Assessment (DPIA) when processing involves high risks to data subjects' privacy.
iii. Regular audits and reviews to assess compliance and ensure that privacy measures are effective.
iv. Training staff on data protection and regularly testing privacy measures.

14 Data Sharing and Transfers

As Data Controllers (Weston Virtual School) we are responsible for ensuring compliance with data protection laws and managing personal data processing activities.

The schools may share personal data with external parties, including:
i). Government Bodies: To comply with legal or regulatory obligations (e.g., educational statistics, government funding).
ii). Service Providers: To support the delivery of educational services (e.g., online learning platforms, IT support, MIS system, Communication).
iii). Examination Bodies: For processing student assessments and qualifications.
iv). Parents/Guardians: To communicate about student progress, welfare, and school events.

Data Processors (third parties working on behalf of the schools) must be chosen based on their ability to meet data protection requirements and have signed data processing contracts.

Contractors, Short-Term, and Voluntary Staff: The School will ensure that these individuals understand and comply with data protection policies when accessing any personal data.

When transferring personal data outside of Kenya, the Schools will ensure that appropriate safeguards are in place to protect the data in accordance with GDPR and the Kenyan Data Protection Act.

15 Data Security Measures

The Institution is committed to safeguarding personal data through a variety of technical and organisational measures, including:
i). Data Encryption: Personal data will be encrypted during storage and transmission to ensure it is protected from unauthorised access.
i**i). Access Control:** Personal data will only be accessible to authorised personnel who require it to fulfil their duties. Role-based access controls will be implemented.
iii). Data Anonymisation: Where possible, personal data will be anonymised to protect individuals' identities when data is used for analysis or reporting.
iv). Data Breach Protocol: The Institution has an established procedure for detecting, reporting, and investigating data breaches. In the event of a breach, affected individuals will be notified, and appropriate authorities will be informed within the required time limit.

16 Data Protection by Design and Default

Weston Virtual School has a duty to consider privacy issues at the design stage of new processes and systems. This includes:
i). Implementing measures to minimize privacy risks.
ii). Ensuring personal data is only processed for specific purposes.
iii). Restricting access to personal data based on the principles of need-to-know.

17 Data Protection Impact Assessment (DPIA)

A DPIA will be conducted when introducing new technologies, processing data, or engaging in large-scale systematic monitoring of publicly accessible areas. This ensures that privacy risks are assessed and mitigated at the earliest stage.

The Data Protection Officer (DPO) at Weston Virtual School will play a critical role in ensuring compliance with data protection laws, including the Data Protection Act 2019 (Kenya) and GDPR. The key responsibilities of the DPO include:
i). Advising the Schools on data protection obligations and monitoring compliance with data protection laws and internal policies.
ii). Conducting training for staff to ensure they understand their data protection responsibilities.
iii). Providing guidance on Data Protection Impact Assessments (DPIAs) for new projects or processing activities that may impact personal data.
iv). Serving as a point of contact for both internal stakeholders and the Office of the Data Protection Commissioner (ODPC) or regulatory authorities.
v). Managing and investigating data protection breaches, ensuring they are reported and addressed promptly.
vi). Promoting a data protection culture within the school by integrating privacy practices into all aspects of operations.

18 Consent
Consent in data protection refers to a data subject's voluntary, informed, specific, and unambiguous agreement to allow their personal data to be processed. Under GDPR and the Kenyan Data Protection Act 2019, consent must meet the following key requirements:
i). Freely Given: Consent must be given without pressure or conditions.
ii). Specific: Consent must be tied to specific purposes for data processing.
iii). Informed: Data subjects must be fully aware of how their data will be used.
iv). Unambiguous: Consent must be expressed through a clear, affirmative action.
v). Revocable: Individuals can withdraw consent at any time.

In Weston Virtual School, consent is required for activities such as processing medical data, using student images or videos for marketing purposes, or sharing data with third parties, and it must be obtained clearly in writing and documented.

19 CCTV and photography
The Schools uses virtual monitoring tools for security and educational integrity purposes. Recordings will be retained for one month and will not be used for other purposes without consent. Written consent will be sought for the use of images or video footage in publications or marketing materials.

20 Storage and Access to Personal Data
Personnel Files: Employee data is kept in the HR department, with access restricted to authorized personnel only.

Pupil Files: Parent and pupil data are stored in the school MIS system. Medical data is maintained by the school nurse or designated health officer.

21 Data Sharing

Personal data may be shared within the schools for legitimate purposes, but new purposes will require a new privacy notice. Data may be shared externally under legal obligations, such as with government institutions, law enforcement agencies, or contractors providing services to the schools.

22 Data Retention and Disposal

Personal data will be retained only for as long as it is necessary to meet the specific purpose for which it was collected. For example, student academic records may be retained for several years after exit from school, while personal contact details may only be kept for the duration of the student's enrolment.

When personal data is no longer required, it will be securely deleted or anonymised. Paper records containing personal data will be shredded, and electronic data will be permanently erased using secure deletion methods.

23 Privacy Notice

The school's privacy notice is available on the official website.

24 Changes to Policy

This policy will be reviewed every two years, or as needed, to ensure ongoing compliance with data protection laws. Any changes to this policy will be approved by the School Leadership Team.