

INSTITUT D'ENSEIGNEMENT SUPÉRIEUR DE RUHENGARI

Accredited by Ministerial Order N° 005/2010/Mineduc of 16 June 2010



Scientia et Lux

DATA PROTECTION POLICY

February 2025



B.P. 155
Ruhengeri
Rwanda
T : +250 788 90 30 30
: +250 788 90 30 32
E : info@ines.ac.rw
W : www.ines.ac.rw

TABLE OF CONTENT

Contents

TABLE OF CONTENT	ii
1. Introduction	1
2. Mission of INES-Ruhengeri.....	1
3. Vision of INES-Ruhengeri	1
4. INES-Ruhengeri 'Core qualities	1
5. Purpose and Scope	2
6. Legal and Regulatory Compliance	2
7. Data Collected	3
8. Data Collection and Use.....	3
9. Consent for Use of Photos and Images	4
9.1. Mechanisms for Obtaining Consent	4
9.2. Handling Consent.....	4
9.3. Withdrawing Consent.....	5
9.4. Mechanisms for Addressing Concerns.....	5
10. Mechanisms for Handling Data Requests	5
10.1. Request for Access	5
10.2. Rectification or Deletion Requests.....	5
10.3. Appeals Process.....	5
11. Data Retention.....	6
12. Data Protection Measures.....	6
13. Roles and Responsibilities	6
14. Third-Party Data Sharing	1
15. Data Breach Response.....	1
16. Monitoring and Review.....	1
17. Budget	2
18. Policy Enforcement and Consequences	2



1. Introduction

INES-Ruhengeri is committed to safeguarding the privacy and security of personal data in compliance with its mission of contributing to national and regional development through specialized university education and research. The institution holds two key certifications: Data Controller and Data Processor, both issued by the Data Protection Office and National Cyber Security Authority of Rwanda. These certifications affirm INES-Ruhengeri's compliance with data protection and cybersecurity standards.

This policy outlines how we collect, use, protect, and manage personal data, ensuring adherence to data protection laws and regulations such as the General Data Protection Regulation (GDPR) and relevant local laws.

2. Mission of INES-Ruhengeri


Contribute through the interactive conjunction between civil society, private sector and public sector to the national and regional development, by providing specialized university education enhanced by research, in order to create competitive enterprises and well paid employment.

3. Vision of INES-Ruhengeri

Universality in each individual; Knowledge in order to unite and better serve the world.

4. INES-Ruhengeri 'Core qualities

The following core qualities lie at the basis of the current performance of INES

<ul style="list-style-type: none"> • Quality • Scientific excellence • Professional consciousness • Flexibility • Innovation • Entrepreneurship • Team spirit • Determination and perseverance • Courage and responsibility <p>By highlighting the core values of a Catholic School and the values of INES Students as listed below, all partners must profit to them</p>	<ul style="list-style-type: none"> • Collaboration (among staff and with students) • Architectural concept • Accessibility (geographical and financial) • Receptivity to local need • Relation with the Catholic Church • Culture of Transparency • Integration of Social Sciences and Communication 
--	---

5. Purpose and Scope

This Data Protection Policy ensures the secure handling of personal data for all stakeholders, including students, staff, faculty, and third-party partners. It applies to all employees, contractors, and agents of INES-Ruhengeri who have access to personal data.

6. Legal and Regulatory Compliance

INES-Ruhengeri complies with all applicable national data protection laws and international regulations, ensuring that all personal data is processed fairly, transparently, and securely.

Mechanisms for Compliance:

Training Programs: All staff and students involved in data handling receive annual training on data protection laws and regulations. **Audits:** Regular internal audits are conducted to ensure compliance with data protection policies and certification requirements. **Certification Maintenance:** The Office of Data Protection at INES-Ruhengeri works with the Data Protection Office and the National Cyber Security Authority to address any compliance gaps.



7. Data Collected

INES-Ruhengeri collects and processes the following categories of personal data: Student Data: Names, contact details, academic records, national ID/passport numbers, photo, health information (where applicable), and payment details. Employee Data: Names, contact details, performance records, photos, payroll information, and other employment-related information. Third-Party Data: Vendor details, partner agreements, and service provider information. Website and IT Data: IP addresses, user login information, and online behavior tracking data collected via cookies and analytics tools. Images and Photographs: Photos and videos taken during INES-Ruhengeri events, lectures, or other official university activities like graduation, anniversaries, and more. Footages or Videos taken by INES CCTV Cameras:

Mechanisms for Data Collection and Usage:

Data Minimization: Only necessary data is collected for specific purposes. Secure Collection Channels: Data is collected via encrypted online forms, secured paper records, and other secure mechanisms to prevent unauthorized access during the collection phase. Data Review: Regular reviews are conducted to ensure the data collected is relevant and up-to-date.

8. Data Collection and Use

Personal data is collected for specific, legitimate purposes, including: Student Administration: Enrollment, course registration, examinations, and maintaining academic records. Employee Management: Recruitment, payroll, and performance evaluations. Research: Data collection for academic research with all necessary permissions and ethical approvals in place. Communication: Informing students, staff, and stakeholders about academic and administrative matters, events, and updates. Promotional Activities: Use of photos and videos of students and staff in marketing materials, on the INES-Ruhengeri website, and across social media platforms (with consent). Footages or Videos taken by INES CCTV Cameras: Footage from INES CCTV cameras is primarily used for security, safety, and institutional integrity, ensuring the protection of students, staff, and property. Access to these recordings is strictly regulated, with only authorized personnel such as campus security, administrative officials, and law enforcement (when legally required) permitted to review them. The use of CCTV footage must comply with data protection and privacy policies, meaning it cannot be accessed, shared, or distributed without proper authorization.



Unauthorized use, including sharing without consent, or using footage for personal or malicious purposes, will result in disciplinary action.

Mechanisms for Processing Data:

Data Access Controls: Only authorized personnel can access sensitive student, staff, and third-party data. **Encryption:** Data is encrypted during storage and transmission to prevent unauthorized access. **Review and Revision:** Periodic reviews of how data is used to ensure it aligns with the purposes for which it was collected. Any data intended for sharing outside of INES-Ruhengeri must go through a formal authorization process to ensure compliance with data protection regulations and institutional policies. A written request must be submitted to the relevant authority, such as the Office of the Data Protection Officer or the university administration, detailing the purpose, recipient, and scope of the data to be shared. Approval will only be granted if the request aligns with legal, ethical, and institutional guidelines, ensuring that sensitive or confidential information remains protected. Unauthorized sharing of data without prior approval may result in disciplinary action, legal consequences, or restrictions on future data access.

9. Consent for Use of Photos and Images

INES-Ruhengeri ensures that proper consent is obtained from individuals (students and staff) before their photos or videos are used for promotional purposes. This section outlines the consent process and mechanisms for handling objections.

9.1. Mechanisms for Obtaining Consent

Initial Notification: Upon joining INES-Ruhengeri, students and staff will be informed about the potential use of their images for promotional purposes via the university's welcome packet or employee/student handbook. **Consent Form:** A clear and specific consent form will be issued to all students and staff, outlining: The type of promotional activities in which their images may be used. The duration of the consent. An opt-in/opt-out option.

9.2. Handling Consent

Signing Consent: Consent will be documented through signed forms, either in print or digitally. **Event-Specific Consent:** Attendees will be notified about photography or videography and asked



for consent via event registration forms or on-site consent stations. Right to Refuse: Individuals have the right to refuse consent without any negative consequences.

9.3. Withdrawing Consent

Request Process: Individuals can withdraw their consent at any time by submitting a written request to the Data Protection Officer (DPO): dpo@ines.ac.rw .Response Time: The DPO will acknowledge receipt of the request within 5 working days and take appropriate steps to stop future use of the individual's image.

9.4. Mechanisms for Addressing Concerns

If a complaint is filed regarding improper use of an image, the DPO will conduct an investigation and take corrective action, such as removing the image from promotional materials.

10. Mechanisms for Handling Data Requests

Individuals have the right to access, rectify, or delete their personal data. The following steps outline the process:

10.1. Request for Access

Submission: Data subjects can submit access requests to the DPO. Verification: The DPO will verify the identity of the individual to prevent unauthorized data disclosure. Response Time: INES-Ruhengeri will provide the requested data within 30 days.

10.2. Rectification or Deletion Requests

Submission: Individuals can request data rectification or deletion. Evaluation: The DPO will assess the validity of the request, ensuring it complies with legal and institutional requirements. Response: Appropriate action, whether data rectification or deletion, will be taken within 30 days.

10.3. Appeals Process

If individuals are not satisfied with the response, they can escalate the issue through the INES-Ruhengeri grievance process or, if necessary, take legal recourse through the Data Protection Office.

11. Data Retention

INES-Ruhengeri retains personal data, including images and videos, only as long as necessary for the purposes for which it was collected or as required by law.

Mechanisms for Data Retention:

Regular Review: Data retention policies are reviewed annually to ensure compliance with legal requirements. Automated Deletion: Where applicable, data is automatically deleted after its retention period has expired unless otherwise required by law or necessary for ongoing projects.

12. Data Protection Measures

INES-Ruhengeri implements a variety of security measures, such as encryption, access control, and regular audits, to protect personal data.

Mechanisms for Security:

Access Controls: Role-based access ensures that only authorized personnel can view sensitive data. Data Encryption: All personal data is encrypted both in transit and at rest. Incident Response: A data breach response team will act immediately to contain, investigate, and report any breaches.

Individuals have the right to: Access their personal data. Correct or delete their personal data.

Withdraw consent for the use of their personal data at any time.

Mechanisms for Exercising Rights:

Submission Form: A standardized form is available on the university website to facilitate data access or correction requests. DPO Review: The Data Protection Officer will review and respond to requests in compliance with relevant laws and regulations.

13. Roles and Responsibilities

The Data Protection Officer (DPO) ensures compliance with this policy and is responsible for addressing any concerns related to personal data usage.





Mechanisms for Compliance:

Quarterly Reports: The DPO submits quarterly reports on data protection activities and any complaints or incidents. **Training:** Mandatory data protection annual training for all staff.

14. Third-Party Data Sharing

Personal data is shared with third parties only when necessary and in compliance with relevant laws.

Mechanisms for Data Sharing:

Third-Party Contracts: All contracts with third-party service providers include specific clauses on data protection responsibilities. **Data Transfer Agreements:** For any cross-border data transfers, INES-Ruhengeri ensures compliance with international data protection laws.

15. Data Breach Response

In the event of a data breach at INES-Ruhengeri, an immediate investigation will be conducted to determine the cause, extent, and impact of the breach. The university will take urgent steps to contain the breach, notify affected individuals and authorities as required by law, and implement corrective measures to prevent future occurrences. If the breach results from negligence, unauthorized access, or intentional misconduct, the responsible party will face strict sanctions, including disciplinary action, suspension, termination of employment or access rights, and potential legal prosecution if the breach violates data protection laws. Additionally, INES-Ruhengeri may impose fines or restrictions on individuals or entities found responsible for compromising institutional data security. In case of a data breach, affected individuals and authorities will be notified as required by law.

Mechanisms for Responding to Data Breaches:

Immediate Containment: Upon discovery of a breach, the incident response team will immediately contain and assess the extent of the breach. **Notification:** Affected parties and relevant authorities will be notified within 72 hours. **Remediation:** INES-Ruhengeri will take corrective measures to prevent future breaches.

16. Monitoring and Review

This policy will be reviewed annually to ensure compliance with evolving legal requirements.

17. Budget

The Data Protection Policy at INES-Ruhengeri will receive an annual budget allocation from the institution to ensure its effective implementation and sustainability. This funding will support essential activities such as staff training on data security, procurement of secure storage systems, regular system updates, and compliance audits. By integrating data protection into the institution's financial planning, INES-Ruhengeri demonstrates its commitment to safeguarding sensitive information and maintaining compliance with relevant regulations. The allocated budget will be reviewed periodically to accommodate emerging data protection needs and technological advancements.

18. Policy Enforcement and Consequences

The data protection policy at INES-Ruhengeri applies to all personal and institutional data collected, stored, processed, or shared within the university, ensuring compliance with privacy laws and ethical standards. It governs the handling of student records, employee information, research data, CCTV footage, and any other sensitive institutional data, protecting it from unauthorized access, misuse, or breaches. All staff, students, and third parties handling such data must adhere to confidentiality guidelines, ensuring that information is only accessed for legitimate academic, administrative, or security purposes. Any violation of the policy, including data leaks, unauthorized sharing, or mishandling of information, may lead to disciplinary actions, legal consequences, or other corrective measures.

Done at INES-Ruhengeri, on 20th February 2025

A handwritten signature in blue ink, appearing to read 'Dr. Mazarati Jean Baptiste'.

Dr. MAZARATI Jean Baptiste

Chairperson of INES-Ruhengeri Governing Body