



Data Protection

Acorns is committed to protecting the privacy and personal data of its students, staff, and families. This policy outlines the principles and procedures that guide the collection, processing, storage, and disclosure of personal data in compliance with the Uganda Data Protection and Privacy Act, 2019.

Inspiring & Empowering

Plot 238 Kisota Road (Along) Northern Bypass Kisaasi Roundabout
+256 393 202 665 | +256 756 202 665 | info@ais.ac.ug | acornsschools.com

Acorns Vision

To inspire and empower each other to achieve our personal best.

Acorns Mission

To build an accessible, inclusive learning community of global citizens that pursues academic excellence in a holistic, inquiry-based environment that develops lifelong learners with the attributes to shape a better and more peaceful world.

Acorns Core Values



IB Learner Profile



IB learner profile

The aim of all IB programmes is to develop internationally minded people who, recognizing their common humanity and shared guardianship of the planet, help to create a better and more peaceful world.

As IB learners we strive to be:

INQUIRERS We nurture our curiosity, developing skills for inquiry and research. We know how to learn independently and with others. We learn with enthusiasm and sustain our love of learning throughout life.	OPEN-MINDED We critically appreciate our own cultures and personal histories, as well as the values and traditions of others. We seek and evaluate a range of points of view, and we are willing to grow from the experience.
KNOWLEDGEABLE We develop and use conceptual understanding, exploring knowledge across a range of disciplines. We engage with issues and ideas that have local and global significance.	CARING We show empathy, compassion and respect. We have a commitment to service, and we act to make a positive difference in the lives of others and in the world around us.
THINKERS We use critical and creative thinking skills to analyse and take responsible action on complex problems. We exercise initiative in making reasoned, ethical decisions.	RISK-TAKERS We approach uncertainty with forethought and determination; we work independently and cooperatively to explore new ideas and innovative strategies. We are resourceful and resilient in the face of challenges and change.
COMMUNICATORS We express ourselves confidently and creatively in more than one language and in many ways. We collaborate effectively, listening carefully to the perspectives of other individuals and groups.	BALANCED We understand the importance of balancing different aspects of our lives—intellectual, physical, and emotional—to achieve well-being for ourselves and others. We recognize our interdependence with other people and with the world in which we live.
PRINCIPLED We act with integrity and honesty, with a strong sense of fairness and justice, and with respect for the dignity and rights of people everywhere. We take responsibility for our actions and their consequences.	REFLECTIVE We thoughtfully consider the world and our own ideas and experience. We work to understand our strengths and weaknesses in order to support our learning and personal development.

The IB learner profile represents 10 attributes valued by IB World Schools. We believe these attributes, and others like them, can help individuals and groups become responsible members of local, national and global communities.

 International Baccalaureate®
Baccalauréat International
Bachillerato Internacional

© International Baccalaureate Organization 2017
International Baccalaureate® | Baccalauréat International® | Bachillerato Internacional®

“IB learner profile”

Table of Contents

Content	Page #
1 Purpose	4
2 Scope	4
3 Definitions	4
4 Principles of Data Protection	4
5 Data Collection	5
• Sensitive Data That Must Be Approved for Collection Before Collection	5
• Approval for Creating a Data Collection Point	6
6 Data Security Measures	6
7 Data Retention of Hard Copy	7
8 Data Subject Rights	7
9 Consent and Confidentiality in Data Sharing	7
10 Third-Party Service Providers	7
• Data Sharing and Transfers	8
11 Campus Regulations and Practices for Data Protection	8
12 Incident Response Plan to Data Breaches	8
13 Compliance and Complaints	9

Data Protection

1 Purpose

Acorns International School (Acorns) is committed to protecting the privacy and personal data of its students, staff, and families. This policy outlines the principles and procedures that guide the collection, processing, storage, and disclosure of personal data in compliance with the Uganda Data Protection and Privacy Act, 2019.

2 Scope

This policy applies to all personal data collected, processed, stored, or shared by Acorns, including data relating to students, families, and staff members.

3 Definitions

Personal data

- Personal data can be anything from basic identity details(name, address, birthday, etc) to more sensitive categories such as health information, biometric data, or financial records.

Authorised Personnel

- Staff who need data for their role. Must have signed a Confidentiality Agreement.

Data Protection Team(DPT)

- Led by the Data Protection Officer/Head of IT(DPO), the other members of the team are the Head of School(HoS), Head of Admissions and Advancement, Head of Human Resources, and Head of Finance. This team is responsible for policy implementation and review. Other members of the Senior Leadership Team may be involved in the DPT as relevant to the incident.
- Data Protection Officer/Head of IT Email: ict@acornskisaasi.com

3rd Party Vendors

- These are individuals who are not Acorns staff members who may work with Acorns to provide services one time or infrequently. They must sign a Confidentiality Agreement.

3rd Party Service Providers / Contingency Staff

- These are individuals who are not Acorns staff members who may work with Acorns to provide services frequently. They must sign a Confidentiality Agreement.

Data Subject

- The person whose data is being collected.

Data Collection Point

- The platform, tool, or process where data is initially gathered from individuals.

4 Principles of Data Protection

Acorns adheres to the following data protection principles:

- Personal data shall be collected and processed lawfully, fairly, and transparently.
- Data shall only be collected for specified, explicit, and legitimate purposes.
- Only necessary and relevant data shall be collected.
- Acorns shall ensure that personal data is accurate and up to date.
- Data shall be retained only as long as necessary for its intended purpose.
- Data shall be protected against unauthorised access, loss, or destruction.
- Acorns shall be responsible for compliance with data protection laws and regulations.

5 Data Collection

Acorns collects personal data through various data collection points, including admission forms, staff records, online platforms, and direct interactions.

Acorns shall only collect or process sensitive personal data such as religious beliefs, political opinions, or health information, if:

- It is required by law.
- Explicit consent is obtained from the data subject.
- It is necessary for the school's legitimate educational or administrative functions.

Before collecting personal data, Acorns shall:

- Inform students, parents, and staff about the purpose and basis for collection.
- Obtain explicit consent where necessary/possible.
- Ensure that data collected is relevant and not excessive.
- Maintain detailed records of data collection activities.
- Conduct policy reviews and practice audits every 2 years to ensure compliance with data protection laws and implementation of practices.

Sensitive Data That Must Be Approved for Collection Before Collection

- Medical conditions and diagnoses
- Mental health information
- Counselling records
- Medications and treatment plans
- Disability information
- Therapy or specialist reports
- Social services involvement
- Court orders
- Family welfare concerns
- Police involvement
- Records of disclosures made by students
- Nationality or immigration status
- Religion or belief
- Gender identity information
- Family circumstances beyond routine emergency contact information
- Custody arrangements
- Financial information
- Parental employment details
- Information about family members' health or personal situations
- Student wellbeing surveys containing personal or sensitive information
- Social-emotional assessments not approved by school leadership
- Fingerprints
- Facial recognition data
- Voice recordings used for identification
- Any other biometric identifiers
- Recordings intended for purposes beyond normal school operations
- Any survey asking students about:
 - Mental health

- Family life
- Religious beliefs
- Political views
- Sexual orientation
- Personal relationships
- Trauma or adverse experiences

Approval for Creating a Data Collection Point

Data collection points could be through a physical form, an online survey, a digital registration form, an application, a verbal interview, or any other medium through which personal, demographic, or other types of information are obtained from data subjects.

Acorns leadership and staff may create data collection points for various purposes; however, all collection must be necessary for the school's legitimate educational, administrative functions and/or child protection.

To create a data collection point, the following steps must be followed:

1. The staff member must send an email to their HoD detailing the purpose of the collection, which information will be collected, and how the information will be used. When possible, the actual form should be supplied.
2. The HoD will review the submission and consider the following:
 - Is the data being collected necessary for legitimate educational, administrative functions and/or child protection?
 - Does the form/document express the purpose of the collection?
 - Does the form/document contain a signature or tick box to indicate explicit consent?
 - Does the form/document contain the following statement:
 - i. "Acorns Kisaasi is committed to protecting the personal data of all students, parents, staff, and stakeholders in accordance with applicable data protection laws. We collect, store, and process personal information solely for educational, administrative, and safeguarding purposes. All data is handled responsibly and securely, ensuring confidentiality and compliance with our Data Protection Policy. By submitting personal information to Acorns International School, Kisaasi, you consent to its use as outlined above."
3. If yes, to all the above, then the data may be collected.
4. If no, the HoD may respond with suggestions for revision or deem the collection unnecessary.
5. Data collected should only be used for the intended purpose and staff must either file the data with their HoD after use, or hand it over for disposal.

6 Data Security Measures

Acorns shall implement appropriate technical and organisational measures to safeguard personal data, including:

- Restricting access to authorised personnel.
- Using secure storage
 - All hard copy files are kept in locked cabinets
 - Online storage connected to the server is securely encrypted
 - All staff and students shall generate unique Google Workspace logins

- Regularly reviewing and updating security protocols.
 - Will be done every 2 years with policy review.
- Implementing multi-factor authentication for access to sensitive data.
- Conducting staff training on data security best practices.
- Establishing an incident response plan to address potential data breaches.

7 Data Retention of Hard Copy

Personal data shall only be retained for as long as necessary to fulfil its intended purpose.

At the end of each academic year, staff are required to clear out their offices/classes and either file data with HoD for keeping, or destroy, or return to the student/family.

Annually, the Data Protection Team will audit information held for 5 years after staff or family members exit. Personal data shall be securely deleted, anonymised or securely archived to prevent unauthorised access.

8 Data Subject Rights

Persons whose data is collected by Acorns have the following rights:

- Request copies of their personal data.
- Request corrections to inaccurate data.
- Request deletion of data no longer needed.
- Object to processing under specific circumstances.
- Object to use of personal data or images for marketing purposes.
- Report any data protection concerns to the school's Data Protection Team.

9 Consent and Confidentiality in Data Sharing

Acorns is committed to maintaining confidentiality and ensuring that personal data is shared only when necessary and with explicit consent. The school shall:

- Clearly communicate the purpose of data sharing and the entities involved.
- Ensure that recipients of shared data adhere to strict confidentiality and data protection standards.
- Implement data-sharing agreements to formalise commitments to safeguarding personal information.

10 Third-Party Service Providers

When students are admitted or staff sign an employment contract, they are agreeing to have data shared with 3rd party providers.

The school maintains a protocol of using 3rd party providers in line with UG law.

3rd party providers will agree to terms and conditions with either their own MOU that aligns with Acorns standards, or with Acorns MOU for Outside Service Providers.

When transferring data outside Uganda, Acorns shall ensure that adequate protection measures are in place, including:

- Ensuring the receiving country has equivalent data protection laws.
- Implementing data transfer agreements that comply with legal requirements.

Data Sharing and Transfers

Acorns shall share personal data with third-party service providers and third-party vendors in cases where:

- Required by law.
- Necessary for the performance of educational or administrative functions.

In order for the above, the recipient MUST provide sufficient guarantees for data security and confidentiality.

This does not apply to information filed about Child Protection and Safeguarding concerns or illegal activities.

11 Campus Regulations and Practices for Data Protection

To enhance data protection on campus, Acorns shall implement the following regulations:

- Restrict access to personal data to authorised personnel.
- Train staff and students to follow proper data handling procedures.
- Mandate the use of school-approved communication channels for sharing sensitive information.
- Require staff to secure all Acorns accounts with passwords and encryption.
- Implement protocols for handling visitor data and access to campus systems.
- Ensure that any video surveillance on campus complies with data protection regulations.
 - Records of video are only available to the IT team, Head of Auxiliary, and the Head of School.
 - If there is a need to review footage, the HoD can make a request to the DPO.
 - In some cases, the footage may be viewed directly by students/staff/family, but only with the approval of the DPO and HoS.
 - Footage is not allowed to be shared directly with students/staff/ families.
 - Footage may be used for disciplinary committees, police cases or other legal action.
- Establish a system for reporting potential data breaches or privacy violations.
- All photos taken by staff shall be uploaded to a secure drive and/or deleted from their personal devices.

12 Incident Response Plan to Data Breaches

In the event of a data breach, the Data Protection Team shall follow the incident response plan to mitigate the impact and restore data security:

- Detects and verifies the occurrence of a data breach.
- Isolate the affected systems to prevent further compromise.
- Determine the extent of the breach, affected parties, and potential risks.
- Alert the relevant authorities, affected individuals, and the National Information Technology Authority - Uganda (NITA-U) as required by law.
- Implement corrective actions to address vulnerabilities and prevent recurrence.
- Maintain records of the breach, actions taken, and lessons learned.
- Conduct a post-incident review and update security measures accordingly.

13 Compliance and Complaints

Acorns has appointed a Data Protection Officer responsible for ensuring compliance with this policy.

Any complaints regarding data privacy should be directed to the Data Protection Officer for resolution. The complaint process includes:

- Submitting a written complaint detailing the concern via email or hand-delivered.
- At least 2 members of the Data Protection Team will review and investigate the complaint.
- The DPT will provide a formal response within 2 weeks from when the complaint was received.
- If the complainant isn't satisfied with the resolution, they are to follow the Communication Policy's Complaint procedure.

Review Committee:

Ibrahim Kawalya, Head of ICT/Data Protection Officer

Jane Namagembe, Chief Operations Officer

Lynn Bugaari Muhangi, Chief Human Resource Officer

Rachelle Hale-Molo, Head of School

Last Reviewed Date: February, 2026

Next Review Date: February, 2028