DATA PROTECTION POLICY

Reviewed:	August 2025
Next Review Due:	August 2026
Applies To:	Whole School
Owner:	Head of School
Approved By:	Vice Chair of Board

Mission, Vision and Values

Mission
To inspire our children to reach their full potential by fostering curiosity and an interest in learning, awakening their minds and illuminating their world.

Vision
To create an affordable international secondary school with a high standard of education where children learn through practical and project-based work. To develop our students' moral and intellectual capacity, and to encourage creativity and adaptability.

Aim
An education that is broad, balanced and challenging, with an emphasis on developing strong connections to our host country, Uganda.

Values
Desire for lifelong learning; an ability to adapt; be innovative and reflective thinkers; open minded, and empathetic while achieving high academic success according to individual potential.

Definitions

For the purposes of this policy, the following terms apply:

Personal Data - Any information relating to an identifiable individual, either directly or indirectly. This includes names, contact details, identification numbers, photographs, assessment records, safeguarding information and digital identifiers.
Processing - Any operation carried out on personal data, including collection, recording, storage, use, sharing, retrieval or deletion.
Data Subject - The individual to whom the personal data relates. Within the school context, this may include students, parents or guardians, staff, contractors, volunteers and visitors.
Data Breach - Any incident in which personal data is lost, accessed, disclosed, altered or destroyed without authorisation.

Scope of Personal Data

Within 7Hills, personal data may relate to:

- Students
- Parents or guardians
- Employees
- Contractors and service providers
- Volunteers
- Visitors
- Any other individuals who interact with the school

Legal Framework

This policy is guided by and complies with:

- The Constitution of the Republic of Uganda
- The Data Protection and Privacy Act, 2019
- The Data Protection and Privacy Regulations, 2021
- Guidance issued by the National Information Technology Authority – Uganda (NITA-U)

This policy also reflects internationally recognised principles of responsible data governance within educational institutions.

Policy Commitment and Compliance

7Hills is committed to:

- Processing personal data lawfully, fairly and transparently
- Protecting the privacy and rights of all individuals
- Ensuring data is handled securely and responsibly
- Maintaining compliance with applicable legal and regulatory requirements

Contents

1. Purpose and Scope

7Hills International School (7Hills) collects and processes personal data so that it can operate effectively as an educational institution, meet its legal and safeguarding duties, and support the wellbeing and progress of students and staff. The school recognises that responsible handling of personal information is essential to maintaining trust, protecting individuals' rights, and ensuring that decisions about data are made carefully, transparently and in the best interests of the community.

This policy sets out the principles, expectations and responsibilities that guide how personal data is collected, stored, used, shared and retained across the school. It applies to all forms of data, whether held on paper, in electronic systems, on personal or school devices, in cloud-based platforms or in photographic and audio-visual formats. The policy applies to all members of the school community who work with data on behalf of 7Hills, including teaching and support staff, leaders, contractors, volunteers and temporary workers.

2. Core Principles of Data Protection

The school's approach to data protection is grounded in the statutory principles that personal data must be handled lawfully, fairly and transparently, collected for clear and legitimate purposes and used only in ways that are relevant and proportionate to those purposes. Data should be accurate where accuracy matters, retained only for as long as it is needed, and protected through appropriate organisational and technical safeguards.

Equally important is the principle of accountability. The school accepts that it must not only comply with legal requirements but also be able to demonstrate that compliance through documentation, reflective review and transparent decision-making. This includes maintaining appropriate records, explaining lawful bases for processing where necessary, and ensuring that staff understand both their responsibilities and the reasons behind them.

3. Governance, Leadership and Responsibilities

Data protection at 7Hills is overseen through a governance structure that combines strategic accountability with clear operational responsibility. The Board of Directors provides high-level oversight, ensuring that information-governance risks are recognised within broader school planning and that sufficient priority is given to legal compliance and the protection of personal data. While the Board does not manage day-to-day implementation, it receives periodic assurance regarding policy application, breaches, emerging risks and areas for improvement.

The Head of School carries executive responsibility for ensuring that data protection is embedded in leadership practice, planning processes and operational systems. Acting as the senior information-risk lead, the Head of School ensures that new systems and initiatives are considered through a privacy-aware lens, that incidents are managed appropriately, and that staff receive guidance and support to understand their obligations.

Independent oversight and professional advice are provided by the Data Protection Officer (DPO), who monitors compliance, advises on risk and complex processing decisions and supports the handling of subject access requests and data-related concerns.

Day-to-day coordination within the school is supported by a designated staff member (academic admin) who ensures requests and incidents are logged, helps staff follow procedures, and acts as a link between departments, leadership and the DPO.

All staff share responsibility for protecting personal data. They are expected to handle information with care, to follow agreed procedures for storage, security and sharing, and to raise concerns promptly if they believe data may have been lost, accessed improperly or used inappropriately. The school supports this expectation through training, communication and a culture that treats data protection as part of everyday professionalism.

4. Lawful Bases for Processing Personal Data

Personal data is only processed by the school where there is a clear, lawful and proportionate reason to do so. In most circumstances, processing takes place because it is necessary for the school to carry out its core public functions as an educational institution, to comply with legal obligations, or to meet reasonable requirements connected with employment or contract arrangements.

Where processing relies on consent, this is used carefully and only where another lawful basis is not appropriate. Consent is obtained in a clear and transparent manner, and individuals are informed that they may withdraw consent at any time. The school recognises that consent must be freely given and meaningful, and that power imbalance in educational settings requires caution.

In situations where the lawful basis or necessity of processing may not be immediately obvious, the school records its reasoning and ensures that the decision aligns with both legal requirements and ethical expectations.

Where further clarity is helpful, particularly when summarising the primary lawful contexts in which the school processes data, these may be expressed as:

- processing required to fulfil the school's public educational duties
- processing necessary to comply with statutory or regulatory obligations
- processing linked to employment and contractual arrangements
- processing undertaken in the school's legitimate interests where reasonable and proportionate

These statements support transparency while remaining grounded in narrative explanation rather than reducing the policy to a checklist.

5. Rights of Individuals

The school recognises that individuals have a range of rights relating to their personal data, including the right to be informed about how their data is used, the right to request access to information held about them, and, in certain circumstances, the right to request restriction, rectification or erasure of data.

Requests relating to these rights may be made verbally or in writing and should be referred promptly to the designated contact so that they can be acknowledged, logged and managed in an orderly and timely manner. The school will normally respond within statutory timescales and will communicate clearly with the requester about any steps required to verify identity or clarify the scope of the request.

The school will normally respond to Subject Access Requests within 30 days, in accordance with the Data Protection and Privacy Act 2019, unless the request is complex or further verification is required.

Where a request is complex, sensitive or may involve competing legal obligations, for example, safeguarding, contractual or examination-related matters, the school will seek advice from the Data Protection Officer before a final decision is made. The emphasis throughout is on fairness, careful judgement and respect for the individual, balanced against the school's wider responsibilities.

In practice, this approach means that:

- requests are handled respectfully and without unnecessary delay
- records of decisions and reasoning are maintained
- confidentiality and safeguarding considerations are considered where relevant

These expectations support consistency while ensuring that the process remains grounded in professional judgement.

6. Data Protection by Design and Impact Assessment

The school adopts a reflective and preventative approach to data protection. When new systems, technologies or processes are introduced, particularly those that involve sensitive information or significant volumes of data, the potential impact on privacy is considered before implementation rather than retrospectively.

Where a proposal is likely to present a higher level of risk, a structured assessment is carried out to examine the nature of the data involved, the necessity and proportionality of the processing, and the potential risks to individuals should something go wrong. This process supports informed decision-making, encourages alternatives to be considered where appropriate, and strengthens overall organisational awareness of privacy implications.

Outcomes of such assessments are recorded and retained, and actions arising from them are reviewed periodically to ensure that controls remain appropriate as systems and circumstances evolve.

7. Data Sharing and Use of Third-Party Services

The school shares personal data with external organisations only where there is a clear and lawful reason to do so. Data sharing may be necessary, for example, to meet statutory reporting duties, to support examination and assessment processes, to enable safeguarding or pastoral support, or to access specialist educational services.

When engaging external service providers or digital platforms that process personal data on behalf of the school, reasonable steps are taken to ensure that those organisations apply appropriate security, confidentiality and compliance standards. Agreements with such providers make clear the limits of data use and the expectations placed upon them.

The school approaches data sharing cautiously and proportionately. Decisions to share are recorded where appropriate, and only the minimum data necessary for the stated purpose is provided.
Where useful for clarity, examples of typical sharing contexts may be referenced, such as:

- statutory reporting to educational authorities or regulators
- approved assessment and examination bodies
- safeguarding or wellbeing partners where legally appropriate

These examples are illustrative rather than exhaustive and are intended to support understanding of the principles that guide sharing decisions.

8. Security, Storage and Access

Protecting personal data from loss, misuse or unauthorised access is a core professional expectation for all staff. The school uses a combination of organisational practice, staff awareness and technical safeguards to reduce the risk of accidental or deliberate data compromise.

Examples of safeguards may include:

- password-protected systems
- role-based access permissions
- encrypted cloud storage
- secure backup procedures
- locked filing cabinets for sensitive paper records

Paper records containing personal information are stored securely when not in use and are not left unattended in public or shared areas. Electronic records are protected through appropriate system permissions and account controls, and portable devices are handled responsibly to minimise the risk of loss.

Access to particularly sensitive information is limited to those who require it for legitimate professional purposes, and staff are encouraged to challenge or seek clarification where they are uncertain about whether information should be shared.

To support consistency, the school reinforces key expectations, including that:

- concerns about potential breaches or data loss are reported immediately
- passwords and accounts are not shared
- personal data is not transferred to unauthorised locations or devices

These expectations complement training and reinforce a culture in which security is understood as part of everyday professionalism.

9. Retention and Disposal of Records

The school retains personal data only for as long as it is needed for legal, operational or educational purposes. Retention periods are informed by recognised guidance for education records and by statutory requirements where they exist. Where no clear external standard applies, a proportionate and reasonable retention period is agreed through leadership consultation.

When records are no longer required, they are disposed of securely and in a manner appropriate to their format and sensitivity. Paper documents are destroyed in a controlled way, while electronic files and storage devices are deleted or wiped to prevent retrieval.

Retention decisions and review processes are documented so that the school can demonstrate that data is not kept indefinitely or without justification.

10. Breach Reporting and Incident Response

Despite safeguards and good practice, errors and incidents may occasionally occur. The school promotes a culture in which staff feel able and are expected to report concerns immediately rather than attempt to resolve them informally or conceal mistakes.

When a potential breach is reported, it is logged and reviewed to establish what has happened, what data may be involved, and whether individuals could be placed at risk as a result. Where appropriate, advice is sought from the Data Protection Officer, and, in serious cases, the Head of School leads the decision-making process regarding regulatory reporting and communication with affected parties.

The emphasis in incident management is on learning, accountability and prevention of recurrence. Following an incident, procedures or systems may be reviewed to strengthen practice.

For clarity in serious cases, responsibilities may be summarised as:

- the Head of School leads strategic decision-making and communication
- the Data Protection Officer advises on risk assessment and regulatory engagement

These summaries assist coordination while remaining embedded within the wider narrative expectations of the policy.

10.1 Data Breach Reporting Timeline

Where a breach presents a significant risk to individuals' rights or safety, the school will consider whether notification to relevant authorities or affected individuals is required within appropriate regulatory time frames.

11. Training, Culture and Professional Awareness

Data protection is sustained not only through systems and documentation, but through professional culture. The school provides induction and periodic refresher guidance to help staff understand their responsibilities and to ensure that expectations remain visible in day-to-day work. Where staff work with particularly sensitive or complex data, additional role-specific guidance may be provided.

Leaders reinforce the message that data protection forms part of ethical and professional conduct rather than being treated as a purely technical or administrative responsibility. Reflection, questions and dialogue are encouraged so that staff feel confident to seek clarification when needed.

12. Monitoring, Review and Policy Ownership

This policy is reviewed regularly to ensure that it remains relevant, compliant and aligned with the operational realities of the school. The review process considers legal developments, organisational change, learning from incidents and emerging best practice.

Findings are shared through leadership structures and, where appropriate, reported to the Board to support governance oversight. Adjustments are made where necessary to strengthen clarity, consistency and effectiveness.

13. Distribution and Access

This policy is available to all staff, students, and parents via the school website and on the school's secure internal digital platform (Google Drive). Printed copies can be requested from the school reception.

14. Related Policies:

This policy should be read in conjunction with other school policies that support responsible information governance, safeguarding and professional conduct. In particular, the following policies provide additional guidance on areas that intersect with data protection:

- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- IT Acceptable Use Policy
- Online Safety / E-Safety Policy
- Records Management and Retention Guidelines
- Recruitment and Safer Hiring Policy
- Photography and Media Consent Policy
- Complaints Policy