BrightEd – Parental Consent Policy & Data Processing Agreement

Effective Date: 04/02/2026

This document supplements the BrightEd Privacy Policy and is intended for use by schools, parents, guardians, and institutional partners. It establishes formal rules for parental consent and defines data protection responsibilities between BrightEd and educational institutions.

PART A: PARENTAL CONSENT POLICY

1. Purpose

The purpose of this Parental Consent Policy is to ensure that the personal and educational data of minors is collected, processed, and stored lawfully, transparently, and securely, with appropriate authorization from parents, legal guardians, or educational institutions.

This policy is designed to meet the expectations of schools and align with:

- Data Protection Act, 2011 (Trinidad and Tobago)
- COPPA (Children's Online Privacy Protection Act)
- GDPR child consent standards
- FERPA-aligned educational oversight

2. Applicability

This policy applies to:

- Students under the age of 18
- All parents or legal guardians of such students
- Schools or institutions acting in loco parentis

3. Consent Models

BrightEd supports the following consent models, depending on institutional preference and legal requirements:

3.1 School-Authorized Consent (Primary Model)

Educational institutions may provide consent on behalf of parents or guardians where permitted by law. In such cases:

- The institution confirms it has obtained required parental authorization
- BrightEd relies on the institution's authority to provision student accounts
- Data is used strictly for educational purposes

3.2 Direct Parental or Guardian Consent

Where required, BrightEd may obtain consent directly from a parent or guardian through:

- Verified email confirmation
- Signed digital consent forms
- Institution-facilitated consent workflows

4. Information Collected from Minors

BrightEd collects only the minimum data necessary to provide educational services, including:

- Student name or identifier
- Grade level or age range
- Academic progress and performance data
- Platform usage for learning analytics

No unnecessary personal, commercial, or behavioral data is collected.

5. Parent and Guardian Rights

Parents and guardians have the right to:

- Review their child’s personal and educational data
- Request correction of inaccurate information
- Request deletion of data, subject to institutional and legal obligations
- Withdraw consent, where applicable

Requests may be made through the institution or BrightEd support channels.

6. Restrictions on Use

BrightEd does not:

- Sell children’s personal data
- Use data for targeted or behavioral advertising
- Permit unauthorized third-party access

All processing is limited to legitimate educational objectives.

7. Data Security for Minors

Enhanced safeguards include:

- Role-based access control
- Encrypted storage of sensitive data
- Monitoring and audit logging
- Limited administrative access

8. Policy Enforcement

Violations of this policy may result in:

- Account suspension or termination
- Institutional review
- Legal or regulatory reporting where required

PART B: DATA PROCESSING AGREEMENT (DPA)

This Data Processing Agreement forms part of any contract between BrightEd and an educational institution (the "Institution").

1. Parties

Data Controller: The educational institution

Data Processor: BrightEd

BrightEd may act as a Data Controller in limited contexts where it independently determines processing purposes.

2. Scope of Processing

BrightEd processes personal data solely for the purpose of providing educational services, including:

- Learning management
- Academic tracking and analytics
- Career pathway modeling
- System administration and support

3. Types of Data Processed

- Student personal identifiers
- Educational records and assessments
- User account credentials
- Platform usage and technical data

4. Processing Obligations of BrightEd

BrightEd agrees to:

- Process data only on documented instructions from the Institution
- Ensure confidentiality of all authorized personnel
- Implement appropriate technical and organizational security measures
- Assist the Institution in fulfilling data subject rights requests
- Notify the Institution of any data breach without undue delay

5. Security Measures

BrightEd maintains safeguards including:

- Encryption in transit and at rest
- Access control and authentication systems
- Regular security audits and updates
- Incident response and recovery procedures

6. Sub-Processors

BrightEd may engage sub-processors (e.g., cloud providers) provided that:

- They are bound by equivalent data protection obligations
- The Institution is informed where required
- BrightEd remains fully liable for their compliance

7. International Transfers

Where data is transferred outside Trinidad and Tobago:

- Appropriate safeguards are implemented
- Transfers comply with the Data Protection Act, 2011 and GDPR where applicable

8. Data Retention and Deletion

Upon termination of services, BrightEd will:

- Delete or return personal data as instructed by the Institution
- Retain data only where legally required
- Provide confirmation of deletion upon request

9. Audits and Compliance

The Institution may:

- Request reasonable documentation of compliance
- Conduct audits subject to confidentiality and security constraints

10. Liability

Each party is responsible for its own compliance obligations under applicable data protection laws.

11. Governing Law

This Agreement is governed by the laws of the Republic of Trinidad and Tobago, unless otherwise agreed in writing.

End of Document