# Bina Bangsa School Academic Data Security and Privacy Policy

## TABLE OF CONTENTS

# 1. Purpose

This policy establishes the framework for ensuring the security and privacy of academic, administrative, and personal data across all Bina Bangsa School (BBS) campuses. It aims to protect the **confidentiality, integrity, and availability** of all digital and physical data, uphold compliance with Indonesian laws (e.g., UU ITE), and foster a secure digital learning environment.

The policy also ensures the proper use of third-party systems, reinforces device-level protection as outlined in the MDM Policy, and secures personal iPad use as defined in the BYOD iPad Student and Parent/Caregiver Acceptable Use Agreement.

---

# 2. Scope

This policy applies to **all BBS campuses** and governs:

- All employees (teachers, staff, leadership)
- All students using school systems or devices
- Third-party vendors and service providers
- All internal and external systems that process or store school-related data
- All personal devices enrolled in school systems (e.g., BYOD iPads)

It encompasses all types of data collected, stored, processed, accessed, transmitted, or disposed of across the institution, including during digital learning and system login monitoring.

# 3. Definitions and Data Subject Rights

### 3.1 Key Definitions

To ensure clarity and consistency, the following terms are defined:

- **Data Security**: Measures and protocols to protect data from unauthorized access, corruption, loss, or breaches.

- **Data Privacy**: The ethical and legal responsibility to collect, use, store, and share data appropriately, especially personal and sensitive data.

- **Sensitive Data**: High-risk data that requires enhanced protection due to potential harm from unauthorized access (see Section 4).

- **IP Address**: A unique numeric identifier assigned to devices accessing internet-based school systems, used for monitoring and detecting anomalies.

- **Archiving**: The secure storage of inactive or historical data for legal or auditing reference.

- **Secure Disposal**: The permanent and irreversible destruction of data (digital or physical) once it is no longer required.

### 3.2 Data Subject Rights

Bina Bangsa School respects the rights of all data subjects (students, staff, parents, and vendors) regarding their personal data.

- **Right to Access**: Individuals may request access to their personal data held by the school.
- **Right to Rectification**: Data subjects may request corrections to inaccurate or outdated information.
- **Right to Erasure**: Personal data may be deleted upon request unless required for legal or academic records.
- **Right to Withdraw Consent**: Individuals can withdraw consent for non-mandatory data collection.

Requests can be submitted in writing to the Head of Educational Technology

# 4. Data Classification

All school-related data is categorized into the following levels:

1. **Public Data**
    - Information intended for public access.
    - Examples: Event announcements, newsletters, published academic calendars.
2. **Internal Data**
    - Information limited to internal users (teachers, staff, students).
    - Examples: Lesson plans, school reports, schedules.
3. **Sensitive Data**
    - Data requiring strict access controls, encryption, and audit trails.
    - Examples:
        - Student and staff personal identifiable information (PII)
        - Academic and assessment data
        - Teacher evaluations and performance reports
        - Disciplinary records
        - Examination/test papers and schemes of work
        - Login IP addresses and system activity logs

All sensitive data must be stored securely (e.g., encrypted Google Drive folders, role-based access, MDM-managed devices).

# 5. Data Collection

- Data collected must be relevant and limited to what is necessary.
- Data collection must comply with **UU ITE** (Undang-Undang Informasi dan Transaksi Elektronik) or any government regulation pertaining to legality of data collection.

- Students' and staff's login IP addresses will be collected for monitoring and security purposes.

# 6. Data Storage and Access

- All sensitive data must be stored in secured systems with role-based access control.
- Examination and test papers, as well as schemes of work, SKs and any files related to the sensitive data, should not be stored on internal servers. These documents must be stored in **Google Drive folders** with sharing restricted to **authorized users by internal email address only**.
- Any internal or external system managing these sensitive documents must utilize **Google Drive API** to handle access and storage, adding another layer of protection even in the event of a security breach.
- For device-level management, refer to the **Bina Bangsa School – Mobile Device Management (MDM) Policy**

## 7. Data Retention and Disposal Policy

This section outlines how Bina Bangsa School (BBS) retains, archives, and securely disposes of data in accordance with legal requirements, operational needs, and best practices.

### 7.1 Data Retention Periods

Different categories of data shall be retained based on their purpose and applicable regulations:

| Data Category | Retention Period |
|---|---|
| Student academic records | Indefinite |
| Student personal information | Indefinite |
| Teacher/staff employment records | Indefinite |
| Examination/test papers & file submission | 2 years |
| Disciplinary records | Indefinite |
| File Drafts (E.g: Exams/Tests) | 1 Year |
| System access and activity logs | 1 Year |

*Note: Where laws or contracts require a longer retention, the longer period will apply.*

### 7.2 Archiving Protocol

- Archived data must be:
  - Encrypted and stored in secured, access-controlled digital archives (e.g., Google Vault, secure drive).
  - Tagged with metadata for easy search, including type, owner, and expiration date.
  - Accessible only to designated personnel (e.g., IT Head, Principals, HR).

### 7.3 Secure Disposal Procedures

Once data exceeds its retention period or is no longer needed, it must be **disposed of securely**:

- **Digital Data Disposal**
  - Files must be permanently deleted from cloud drives and backups using secure delete protocols (e.g., Google Workspace data deletion, disk wiping).
  - External systems must use built-in secure delete features.
  - IT must confirm no recoverable copies remain.
- **Physical Data Disposal**
  - Printed sensitive documents must be shredded using a cross-cut shredder or disposed of via secure document disposal services.
  - Obsolete storage devices (USBs, HDDs) must be degaussed, physically destroyed, or wiped.

### 7.4 Responsibilities

- **IT Department** is responsible for:
    - Managing retention schedules for digital systems
    - Automating alerts and deletion processes when possible
    - Logging disposal actions for audit purposes
- **Academic, HR, and Admin Units** are responsible for:
    - Identifying obsolete documents under their custody
    - Coordinating with IT or secure disposal vendors for deletion or shredding

### 7.5 Exceptions and Holds

- Data subject to **investigation, litigation, audit, or legal request** must not be deleted, even after its retention period has passed.
- Such data will be placed on **legal hold** by the IT Department or relevant authority, and disposal will resume only after clearance.

# 8. Password Policy and Login SOP

### 8.1. Password Change Protocol

- All teachers are required to change their passwords at the start of every term.
- Default password should be following the Password Strength Requirements in Section 8.2
- Internal or external systems should prompt automatic password change upon login during the first week of every term.

### 8.2. Password Strength Requirements

- Minimum 8 characters
- Must include uppercase, lowercase, number, and special character
- Should not include easily guessable patterns like birth dates or simple sequences

### 8.3. Forgotten or Compromised Passwords

- Users must immediately report to the IT Department if they suspect password compromise.
- Password resets can only be facilitated through official channels.

### 8.4. Account Lock Policy

- After 3 unsuccessful login attempts, accounts will be temporarily locked for 15 minutes.
- Persistent lockouts will be red flagged to the system administrator for review.

### 8.5. OTP (One-Time Password) Policy

- OTP is mandatory for system login from new or unrecognized devices and locations.
- OTP codes will be sent to the user’s registered school email.
- OTP expiration is set to 5 minutes.
- Users must not share OTPs with anyone. Any breach must be reported immediately.
- Systems must be configured to allow OTP regeneration with rate-limiting to prevent abuse.
- Failed OTP authentication will send email alerts for registered email.
- OTP resend requests can only be done once.

### 8.6. Responsibility

- Users are responsible for keeping their credentials and OTP confidential.
- Misuse or negligence leading to unauthorized access will be subject to disciplinary action.

### 8.7 Student Security Awareness

Digital security expectations are embedded in the Computer Science and Form Class Time curriculum. See: Bina Bangsa School Digital Citizenship Program

# 9. Data Backup

- The database and file systems are **backed up daily**.
- Backups must be stored securely in a location separate from the main system.
- The system must allow **full restoration at any time** in case of data corruption, accidental deletion, or cyberattack.

# 10. Third-Party Vendor Requirements

- All third-party vendors handling BBS data must:
    - Sign a **Data Protection Agreement.**
    - Provide a **Red Flag Viewer** and alert system to detect and report unusual login activity such as:
        - Students accessing other students' accounts.
        - Students accessing teacher, principal, academic board, or other staff accounts.
        - Teachers accessing other teachers' or staff accounts.
        - Any login behavior that deviates from normal usage patterns or geographic/IP inconsistencies.
    - Comply with this Data Security and Privacy Policy.
    - Server should be available 24/7

# 11. Data Sharing

All systems that manage or store sensitive data (e.g., academic records, examination papers, personal and disciplinary information) must maintain **comprehensive audit logs** that record both **login events** and **user activity** during each session.

- Sharing of sensitive data via unsecured methods (e.g., personal email, public drives) is strictly prohibited.
- Access to sensitive data must be **logged and auditable**.
- All students using personal iPads must comply with the **BYOD iPad Student and Parent/Caregiver Acceptable Use Agreement**, which outlines acceptable behavior, security responsibilities, and monitoring expectations

### 11.1 Minimum Logging Requirements

Each access log must include the following:

- **User ID or email address**
- **Login timestamp and logout timestamp**
- **IP address and device information**
- **Session duration**
- **Menu or section accessed** (e.g., "Exams > JC1 Mathematics > Upload Paper")
- **Actions performed** (e.g., viewed, edited, downloaded, shared, deleted)
- **Attempted unauthorized actions** (e.g., trying to access restricted files)

### 11.2 Storage and Security of Logs

- Logs must be:
  - Stored securely on a protected server or cloud platform with encryption at rest
  - Backed up daily
  - Retained for at least **12 months** for all systems containing sensitive data
  - Configured to be **tamper-proof** or write-only to preserve forensic integrity

### 11.3 Review and Monitoring

- The **IT Department** is responsible for:
    - Ensuring logging is activated on all critical platforms (e.g., Google Workspace Admin Console, AIS or 3rd party providers applications)
    - Conducting **monthly log reviews** to detect unusual patterns or unauthorized access
    - Flagging red-flag behaviors such as:
        - Access to exam papers outside of work hours
        - Attempted file downloads from unauthorized roles
        - High-frequency access to sensitive menus in a short time
        - Location/IP mismatch alerts

- The **Head of Educational Technology** or assigned auditor will:
    - Receive a **quarterly summary** of access patterns and red-flag incidents
    - Lead investigations when anomalies or breaches are reported
    - Coordinate with leadership or disciplinary committee when further action is required

### 11.4 User Notification and Transparency

- Staff and students are notified that system usage and actions are logged for safety and integrity.

- All logs will only be accessed by **authorized personnel** for the purpose of security, auditing, and incident investigation.

# 12. Incident Response

- Any suspected or actual data breach must be reported to the IT department immediately.
- Affected users must be notified, and containment measures must be initiated within 24 hours.

### 12.1 Containment Protocol for Hacking or Illegal Access

In the event of hacking or illegal system access:

1. **Immediate Action:**
   - IT will disable the affected user accounts.
   - Force logout of all current sessions.
   - Revoke all external API tokens, if applicable.
2. **Isolation:**
   - Temporarily disconnect affected systems from the network to prevent spread.
3. **Investigation:**
   - Collect access logs, IP history, and any suspicious login records.
   - Assess affected data types and scope of exposure.
4. **Recovery:**
   - Restore from the latest secure backup if data has been altered or deleted.
   - Require affected users to reset their passwords.
5. **Reporting:**
   - A detailed incident report must be submitted to school leadership.
   - Notify impacted users, if necessary.
6. **Review and Prevent:**
   - Update system rules, alerts, or firewall policies.
   - Re-assess access permissions and vendor integrations.

### 12.2 Breach Notification Timelines

In accordance with transparency and accountability:

- All confirmed data breaches must be reported to affected individuals within **72 hours**.
- The school leadership and EdTech team must notify any regulatory bodies if required under Indonesian or international law.
- Initial internal containment must occur within **24 hours** of detection.

# 13. IP Address Collection and Consent

## 13.1 Purpose

To detect unauthorized access and academic dishonesty, BBS collects the IP address used by staff and students when logging into school systems.

## 13.2 Usage

This data is solely used for:

- Monitoring suspicious login activity
- Investigating security incidents
- Supporting academic integrity

## 13.3 Data Protection

- No personal browsing data is collected.
- IP address logs are stored securely and accessed only by authorized personnel.

## 13.4 Parental Consent for IP Address Tracking

Before enabling IP tracking for student accounts, the school must distribute a **Parental Consent Letter** and obtain signed approval. This letter explains the importance of IP tracking for digital safety and preventing unauthorized access. Without this consent, the student's login data may not be monitored. Sample letter

---

# 14. Artificial Intelligence (AI) Use

Teachers and students must refer to the official **BBS AI Guidelines** before using any AI tools or services in their academic or administrative tasks.

Link: BBS AI Guidelines

# 15. Penetration Testing and Vulnerability Management

## 15.1 Hiring of Penetration Tester

Bina Bangsa School may hire a certified penetration tester on a project basis to assess the security of both internal and external systems. The role of the penetration tester includes but is not limited to:

- Conducting authorized simulated cyberattacks to test the strength of our security systems
- Identifying security vulnerabilities in software, infrastructure, or configurations
- Assessing the risk level of vulnerabilities discovered
- Preparing a detailed report of findings and recommendations
- Advising on best practices to mitigate future threats

## 15.2 Obligation to Remediate

- All internal system teams and third-party providers are required to fix vulnerabilities identified in the penetration tester’s report.
- **Critical vulnerabilities** must be patched **immediately upon receipt of the report**.
- All other vulnerabilities must be resolved within **48 hours** from the time the report is received.
- Delays in patching must be escalated to the EdTech and Leadership teams for further action.

## 15.3 Verification

- Follow-up scans or re-testing may be conducted by the penetration tester to confirm that issues have been fully resolved.

## 15.4 Confidentiality and Ethics

- The penetration tester will operate under strict confidentiality agreements and adhere to ethical guidelines in handling school data.

### 15.5 Audit and Compliance Schedule

To ensure compliance with this policy:

- Internal audits of data access logs and policy compliance will occur **twice annually**.
- Penetration testing results will be reviewed as part of each audit.
- An  audit team will be formed at least **once every two years**.
- Audit reports will be reviewed by the Leadership Team and filed by the Head of Educational Technology.

## 16. Training and Awareness

- All staff will receive annual training on data security and privacy protocols.
- New staff must complete a data security induction.

## 17. Policy Enforcement

All members of the Bina Bangsa School community — including teachers, staff, students, administrators, and third-party vendors — are expected to comply fully with this Data Security and Privacy Policy, as well as related digital use agreements (e.g., MDM, BYOD, and AI guidelines).

### 17.1 Accountability

- **All Users** are responsible for:
  - Following data access and sharing protocols.
  - Maintaining password confidentiality and device security.
  - Reporting suspected data breaches or unauthorized access immediately.
- **School Leadership & EdTech Department** are responsible for:
  - Monitoring compliance through audits, system logs, and usage reports.
  - Investigating reports of policy violations.
  - Enforcing disciplinary actions when necessary.

## 17.2 Violations and Consequences

Violations of this policy include, but are not limited to:

- Unauthorized access to sensitive data (e.g., student grades, exams)
- Sharing confidential files via unsecured channels
- Circumventing or removing Mobile Device Management (MDM) controls
- Ignoring password policies or OTP requirements
- Misuse of AI tools in ways that compromise privacy or academic integrity
- Failure to securely dispose of academic data past its retention period

Depending on the severity of the violation, consequences may include:

- **For Students**: Warning, restricted access to school systems, parent notification, academic sanctions, suspension, or expulsion.
- **For Staff or Teachers**: Warning, loss of access privileges, performance review, suspension, or termination.
- **For Vendors**: Termination of contracts, legal reporting, and denial of future engagements.

## 17.3 Investigation and Disciplinary Process

- All suspected violations will be documented and reviewed by the **IT Department**, **Academic Leadership**, and **Disciplinary Committee** (as appropriate).

- Investigations will involve:

  - Review of system logs and access records
  - Interviews with relevant parties
  - Forensic inspection of devices or platforms if needed

- A report will be submitted to School Leadership outlining findings and recommended actions.

- The accused party will be given an opportunity to respond before disciplinary decisions are finalized.

### 17.4 Appeals

- Students and staff have the right to appeal disciplinary actions through the school's grievance process.
- Appeals must be submitted in writing within 5 working days of the disciplinary notice.

## 18. Policy Review

- This policy will be reviewed annually by the IT and Leadership Team.

### 18.1 Policy Version Control

| Version | Date | Description |
|---|---|---|
| 1.0 | 01-Aug-2025 | Initial release |

## 19. Contact

Questions or concerns should be directed to the Head of Educational Technology at headofedtech@binabangsaschool.com

## 20. Related and Linked Documents

The following documents and resources are referenced in this policy:

| No. | Document Name | Description | Link |
|---|---|---|---|
| 1 | **MDM Policy** | Guidelines for Mobile Device Management in BBS | Link |
| 2 | **BYOD iPad Student and Parent/Caregiver Acceptable Use Agreement** | Rules and monitoring expectations for personal iPad usage | Link |
| 3 | **Digital Citizenship Program** | Curriculum module for digital behavior and awareness | Link |
| 4 | **AI Guidelines** | Official school guidance on acceptable AI use | Link |
| 5 | **Data Protection Agreement** | Bina Bangsa School Third-Party Data Protection Agreement (DPA) | Link |
| 6 | **Ip Address Collection Letter to Parents** | Parental Consent for IP Address Collection of Student Logins in our School System | Link |