

## **I. POLICY STATEMENT**

Arkansas Baptist College (“the College”) is committed to safeguarding the privacy, confidentiality, and integrity of personal and institutional data. This policy establishes the standards and responsibilities for the collection, use, storage, protection, and retention of data in compliance with applicable federal and state laws and best practices in higher education.

---

## **II. PURPOSE**

The purpose of this policy is to ensure that Arkansas Baptist College maintains appropriate administrative, technical, and physical safeguards to protect personal data and institutional information, while supporting the College’s academic, administrative, and operational functions.

---

## **III. SCOPE**

This policy applies to all Arkansas Baptist College students, employees, contractors, and any individuals or entities who access, use, or manage College data or information systems.

---

## **IV. DEFINITIONS**

### **Data**

Information in a format that can be processed by Arkansas Baptist College systems, including electronic and physical records.

### **Personal Data**

Any information relating to an identifiable individual, including but not limited to students, employees, applicants, and alumni. This includes identifiers such as names, identification numbers, email addresses, location data, online identifiers (e.g., IP addresses), or other characteristics specific to an individual.

### **Data Subject**

Any individual whose personal data is collected, maintained, or processed by Arkansas Baptist College.

### **Consent**

A freely given, specific, informed, and unambiguous indication of a data subject’s agreement to the processing of their personal data.

### **Data Storage**

The methods and systems used by Arkansas Baptist College to securely retain and manage data in electronic or physical formats.

---

## **V. POLICY REQUIREMENTS**

### **A. Baseline Requirements**

1. All employees and authorized users must protect College data by following established security policies and procedures.
2. Data shall not be shared informally and must only be accessed based on assigned roles and responsibilities.
3. Arkansas Baptist College shall provide training and guidance to ensure employees understand their data protection responsibilities.
4. Personal data shall not be disclosed to unauthorized individuals within or outside the College.

---

### **B. Data Collection**

1. Arkansas Baptist College collects personally identifiable information (PII) that is voluntarily provided through institutional processes, including admissions, financial aid, course registration, employment, and other College services.
2. The College shall limit data collection to only what is necessary to fulfill legitimate institutional purposes.

---

### **C. Data Protection**

1. The College shall implement reasonable administrative, technical, and physical safeguards to protect personal data.
2. While the College strives to protect all data, no system of transmission or storage can be guaranteed to be completely secure.
3. The College is not responsible for the privacy or security practices of third-party systems not controlled by Arkansas Baptist College.

---

### **D. Data Retention**

1. Personal data shall be retained only for as long as necessary to meet operational, legal, and regulatory requirements.
-

## **E. Data Use and Disclosure**

1. Personal data may be used to support College operations, provide services, and communicate with students, employees, and stakeholders.
  2. Arkansas Baptist College does not sell or trade personal data.
  3. Personal data may be disclosed only under the following conditions:
    - With the explicit consent of the individual;
    - As required by law, court order, or legal process;
    - To authorized service providers acting on behalf of the College, provided they agree to maintain confidentiality and data security.
  4. Individuals may request removal of non-essential or outdated contact information, when appropriate, through the Office of the Registrar (students) or Human Resources (employees).
  5. Use of Arkansas Baptist College information systems constitutes acknowledgment and consent to the data practices outlined in this policy.
  6. Aggregated, non-identifiable data may be used for institutional improvement, analytics, and security monitoring.
- 

## **F. Data Storage**

1. All electronic data must be securely stored and protected against unauthorized access, loss, or cyber threats.
  2. Data must be stored on approved Arkansas Baptist College systems, including designated servers and authorized cloud services.
  3. Storage of institutional data on personal devices is prohibited unless explicitly authorized and properly secured.
  4. Physical records containing sensitive information must be secured in locked or restricted-access locations when not in use.
- 

## **VI. RESPONSIBILITIES**

- **Office of Information Technology**  
Responsible for implementing and maintaining data security systems and protocols.

- **Faculty and Staff**  
Responsible for safeguarding data and complying with all provisions of this policy.
  - **Supervisors and Department Leaders**  
Responsible for ensuring that employees understand and comply with this policy.
- 

## **VII. COMPLIANCE**

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or dismissal, in accordance with Arkansas Baptist College policies and procedures.

---

## **VIII. RELATED POLICIES**

- Acceptable Use Policy
  - Records Retention Policy
  - Information Security Policy
  - Family Educational Rights and Privacy Act (FERPA)
- 

## **IX. REVIEW AND REVISION**

This policy shall be reviewed periodically by the Office of Information Technology and College leadership and updated as necessary to remain compliant with applicable laws and institutional needs.