China New Higher Education Group
Data Protection Policy

I. General Provisions

(I) Purpose of the Policy

This Policy is formulated in accordance with relevant laws and regulations to regulate data processing activities of all information systems of the Group, protect the security of users' personal information and privacy rights and interests, and prevent data security risks.

(II) Scope of Application

This Policy applies to all data processing activities involved in the operation, maintenance and management of information systems of the Group and its affiliated schools.

(III) Basic Principles

1. Principle of Legitimacy and Legitimacy - Data processing shall have a clear and reasonable purpose and adopt methods that have the minimal impact on personal rights and interests.

2. Principle of Minimal Necessity - Only the minimum necessary personal information shall be collected. Any excessive collection is prohibited.

3. Principle of Openness and Transparency - Data processing rules shall be disclosed to users and subject to active supervision.

4. Principle of Security Assurance - Necessary measures shall be taken to prevent the leakage, tampering and loss of personal information.

II. Data Storage Security

(I) Storage Environment Requirements

Servers of all information systems shall be deployed in IDC computer rooms or cloud service environments that meet national standards.

1. All user data shall be stored within the territory of China and shall not be transmitted or stored overseas.

2. Reliable storage media shall be adopted, and regular inspections shall be conducted on the health status of equipment.

(II) Data Backup and Recovery

1. Regular data backup shall be implemented, and backup data shall be stored on independent storage devices and encrypted.

2. Off-site backup shall be implemented for important data to prevent regional disaster risks.

III. Data Sharing and Transmission

(I) Internal Sharing

Data connection and sharing among various information systems shall comply with the following requirements:

1. Only fields necessary for business operations shall be shared, and full-database sharing is prohibited.

2. Encrypted channels shall be adopted for data transmission, using SSL/TLS or VPN technologies.

3. Data sharing logs shall be recorded and retained for no less than six months.

(II) Third-Party Sharing

Data sharing with third parties shall comply with the following requirements:

1. Third-party service providers with corresponding qualifications and security capabilities shall be selected.

2. When signing business cooperation agreements, the data protection obligations and liability for breach of contract of the third party shall be clearly specified.

3. Regular reviews shall be conducted on the data protection measures of third parties.

(III) Cross-Border Data Transfer

In principle, user data shall not be transmitted overseas. If it is indeed necessary to provide data overseas under special circumstances, a security assessment by the national cyberspace administration shall be conducted, and users shall be informed and their consent obtained.

IV. Technical Security Measures

(I) Access Control

1. A unified identity authentication mechanism shall be implemented, and users may only access the corresponding information systems after identity verification.

2. Role-Based Access Control (RBAC) shall be implemented, and permissions shall be assigned in accordance with the principle of least privilege.

(II) Network Security

1. Firewalls shall be deployed to restrict unnecessary network access, and network isolation shall be implemented.

2. Intrusion detection or intrusion prevention systems shall be deployed, and regular vulnerability scans shall be conducted.

(III) Application Security

The Security Development Lifecycle (SDL) shall be followed, and strict verification and filtering shall be conducted on user input to prevent SQL injection, XSS, CSRF and other attacks.

(IV) Data Transmission Security

1. The HTTPS protocol (TLS 1.2 or later) shall be used for all network transmission.

2. Encrypted channels shall be used for connection with third-party systems.

(V) Security Monitoring and Auditing

1. Key operations such as user login, data access, data modification and permission change shall be recorded.

2. Real-time monitoring and alerting shall be conducted on abnormal behaviors. The integrity of audit logs shall be protected.

V. Management Security Measures

(I) Organizational Management

1. A Data Security Management Team of China New Higher Education Group shall be established to clarify the division of data protection responsibilities and regularly review the effectiveness of security management measures.

2. A Data Protection Specialist shall be appointed to be responsible for the daily management of data protection.

(II) Personnel Management

1. All staff who may have access to user data shall sign a Confidentiality Agreement.

2. Background checks shall be conducted on key position personnel. All system permissions shall be revoked immediately upon an employee's resignation.

(III) Supplier Management

1. Due diligence shall be conducted on third-party service providers to assess their data protection capabilities.

2. Agreements shall be signed to specify the data protection obligations of service providers, and regular reviews shall be conducted on their data protection measures.

(IV) Risk Assessment

Special assessments shall be conducted before the launch of new functions and major changes, and response measures shall be formulated for identified risks.

(V) Emergency Response

In the event of a data security incident, the emergency response plan shall be activated immediately, remedial and control measures shall be taken, a report shall be made to the competent authority in accordance with the law, and affected

users shall be notified in a timely manner. At least one data security emergency drill shall be organized every year, and full-staff security awareness training shall be conducted regularly.

VI. Supplementary Provisions

(I) Right of Interpretation

The Smart Digital Center of China New Higher Education Group shall be responsible for the interpretation of this Policy.

(II) Effective Date

This Policy shall come into force on the date of issuance.

China New Higher Education Group Ltd.

March 10, 2026