ALUMNI-Ready Privacy Policy

Effective Date: 11 May 2026
Last Updated: 11 May 2026

1. Introduction

This Privacy Policy explains how AppliedHE Pte. Ltd. (“AppliedHE”, “we”, “us”, or “our”) collects, uses, discloses and protects personal data through the ALUMNI-Ready platform (the “Platform”), accessible at https://alumniready.com and through custom domains operated by participating universities.

We are committed to handling personal data in accordance with the Personal Data Protection Act 2012 of Singapore
(the “PDPA”) and applicable regulations issued by Singapore’s Personal Data Protection Commission (“PDPC”).

This Policy applies to individuals who interact with the Platform, including alumni members, students, university administrators, staff users, prospective university clients and visitors to our public website.

2. Who We Are

ALUMNI-Ready is a product of AppliedHE Pte. Ltd., a company incorporated in Singapore.

Legal Entity: AppliedHE Pte. Ltd.

Registered Office: 7 Temasek Boulevard #12-07 Suntec Tower One, Singapore 038987

Email: info@appliedhe.com

Website: https://alumniready.com

For the purposes of the PDPA, AppliedHE may act in two different capacities:

As an Organisation

AppliedHE acts as an Organisation when it collects personal data directly through its own public website, for example through enquiry forms, registrations of interest, event sign-ups, contact forms or communications from prospective University Clients.

As a Data Intermediary

AppliedHE acts as a Data Intermediary when it operates a University Client’s branded instance of the Platform. In this role, AppliedHE provides software-as-a-service infrastructure that the University Client uses to manage its alumni community. The University Client remains responsible for determining what personal data is collected, how it is used, who it is disclosed to, how long it is retained and how requests from individuals are handled.

If you are an alumnus, student, staff member or invited user of a university using the Platform, your personal data within that university’s Platform instance is controlled by your university and not by AppliedHE. You should refer to your university’s own privacy notice for details on how your personal data is collected and used.

AppliedHE does not access, view or use Customer Data in the ordinary course of operating the Platform, except where necessary for technical support, security, maintenance, legal compliance or as instructed by the relevant University Client.

3. Personal Data Processed Through the Platform

This section describes the categories of personal data that may be processed through the Platform.

For personal data within a University Client’s Platform instance, the data is collected by and remains under the control of the relevant University Client. AppliedHE processes that data only as a Data Intermediary by hosting, storing, transmitting, securing and supporting the Platform.

For personal data submitted directly to AppliedHE through our own public website, AppliedHE acts as the Organisation and handles that data in accordance with this Policy.

3.1 Data You Provide Directly

When you register, sign in, complete your profile or use the Platform, you may provide:

Identification and contact data, such as full name, email address, phone number and mailing address.

Academic data, such as graduation year, faculty, department, programme of study and student ID where provided

by your university.

Professional data, such as employer, job title, industry and professional location.

Profile data, such as profile photo, biography and links to professional or social media profiles.

Authentication data, such as password, which is stored as a one-way cryptographic hash. We do not store passwords in readable form.

Communications, such as messages, posts, comments, group discussions, news submissions and success stories.

Event and membership data, such as event registrations, ticket purchases, membership selections and RSVP responses.

Job board data, such as job listings, applications and related information submitted through the Platform.

Custom fields, which may include additional information collected through forms configured by your University Client.

3.2 Data Provided by Your University

Your University Client may upload, import or create personal data about you in the Platform, including through bulk uploads, CSV files, alumni records, student information systems or other institutional databases.

This may include the categories listed above and any other data the University Client determines is necessary for its alumni engagement activities.

The University Client is responsible for ensuring that it has the lawful basis, authority and consent required to upload and process such data through the Platform.

3.3 Data Collected Automatically

When you use the Platform, certain information may be collected automatically, including:

Technical data, such as IP address, browser type, browser version, device type, operating system and time zone.

Usage data, such as pages visited, features used, time spent, links clicked and login timestamps.

Cookie and session data, as described in Section 13.

3.4 Sensitive Personal Data

AppliedHE does not intentionally collect special categories of sensitive personal data, such as health information, religious beliefs, political opinions or similar sensitive information.

If a University Client configures the Platform to collect sensitive personal data, the University Client is solely responsible for ensuring that it has a lawful basis, proper consent and appropriate safeguards for doing so.

AppliedHE is not responsible for the University Client’s decision to collect sensitive personal data through custom fields, forms or user submissions.

4. How Personal Data Is Used

Most user-facing uses of personal data within the Platform are determined by the relevant University Client. These may include alumni communication, event invitations, membership management, fundraising appeals, community engagement, networking, job postings and reporting.

AppliedHE does not decide these uses. AppliedHE processes personal data only as necessary to provide, maintain, secure and support the Platform.

AppliedHE may process personal data for the following purposes:

Operating the Platform

To store, transmit, display and process personal data within the Platform as configured by the University Client.

Authentication

To verify logins, support account access, enable password recovery and protect user accounts.

Security

To detect fraud, abuse, unauthorised access, malware, suspicious activity and other threats to the Platform.

Technical Support

To respond to technical issues raised by University administrators, including accessing limited data only where necessary and where reasonably required to resolve the issue.

Service Operation and Improvement

To diagnose technical issues, fix bugs, maintain backups, improve Platform performance and enhance features. Where possible, AppliedHE uses aggregated or anonymised data that does not identify individuals.

Legal and Regulatory Compliance

To comply with applicable laws, regulations, court orders, lawful requests and regulatory obligations.

AppliedHE does not:

Sell, rent or trade personal data.

Use Customer Data for AppliedHE's own marketing or advertising.

Use Customer Data to build individual profiles outside the Platform.

Use Customer Data to train artificial intelligence or machine learning models.

Access Customer Data except where necessary for service operation, support, security, legal compliance or as instructed by the University Client.

Use Customer Data for purposes unrelated to providing and supporting the Platform.

5. Legal Bases for Processing

AppliedHE relies on lawful bases recognised under the PDPA and applicable law, including:

Consent

Where you provide consent, such as for direct communications from AppliedHE.

Deemed Consent by Contractual Necessity

Where processing is reasonably necessary to provide the Platform or services requested by a University Client.

Legitimate Interests

For security, fraud prevention, system integrity, account protection and prevention of misuse.

Legal Obligation

Where processing is necessary to comply with applicable laws, regulations, court orders or lawful requests.

For data controlled by a University Client, the University Client is responsible for identifying and maintaining the appropriate lawful basis for processing.

6. How We Disclose Personal Data

AppliedHE does not sell personal data.

AppliedHE may disclose personal data only where necessary and in limited circumstances, including:

To the relevant University Client

The University Client has access to the personal data held in its Platform instance. This is the central purpose of the Platform.

To authorised Platform users

Information you publish to your profile, community feed, groups, events, job boards or other shared areas may be visible to other authorised users within your University Client's Platform instance, depending on Platform settings and privacy controls.

To infrastructure and hosting providers

The Platform is hosted using third-party infrastructure providers, including DigitalOcean LLC, with data hosted in Singapore.

To professional advisers

We may disclose data to lawyers, auditors, accountants, insurers or other professional advisers where reasonably necessary and subject to confidentiality obligations.

To comply with law

We may disclose data where required by law, regulation, court order, government authority, regulator or lawful request.

To protect rights and security

We may disclose data where necessary to protect the rights, property, safety, security or integrity of AppliedHE, the Platform, University Clients, End Users or others.

In a corporate transaction

We may disclose data in connection with a merger, acquisition, restructuring, financing, sale of assets or transfer of business, subject to reasonable safeguards.

Where a University Client connects its own third-party services, such as payment gateways, email delivery tools, analytics tools or external databases, the University Client is responsible for that third-party relationship and the handling of any data shared with that third party.

AppliedHE is not responsible for third-party services selected, configured or used by the University Client.

7. Data Hosting and Cross-Border Transfers

Personal data processed through the Platform is currently stored on servers located in Singapore, hosted by DigitalOcean LLC.

AppliedHE does not routinely transfer Platform personal data outside Singapore. If cross-border transfer becomes necessary in the future, AppliedHE will take reasonable steps to ensure that the recipient is bound by legally enforceable obligations providing a standard of protection comparable to the PDPA, in accordance with the Transfer Limitation Obligation under Section 26 of the PDPA.

Where a University Client chooses to connect external third-party services, the University Client is responsible for assessing and managing any cross-border transfer associated with those services.

8. Security

AppliedHE uses reasonable technical and organisational measures to protect personal data against unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

These measures may include:

Encryption of data in transit using TLS.

One-way hashing of authentication credentials.

Multi-factor authentication availability for administrator accounts.

Logical data isolation between University Client instances.

Role-based access controls.

Least-privilege access principles.

Audit logging of administrative actions.

Security updates and dependency patching.

Restricted access to production systems.

Internal policies for staff handling of personal data.

However, no system, network, software or method of transmission can be guaranteed to be completely secure, uninterrupted or error-free.

The University Client and End Users are responsible for maintaining the security of their own accounts, passwords, devices, systems and networks.

If you believe your account has been compromised, please contact your University Client and AppliedHE promptly.

9. Data Breach Response

AppliedHE applies commercially reasonable measures to reduce the risk and impact of security incidents. However, personal data breaches may occur despite reasonable safeguards.

In the event of a suspected or confirmed personal data breach affecting the Platform, AppliedHE will take reasonable steps to:

Contain the incident.

Preserve relevant evidence.

Investigate the cause and scope of the incident.

Notify the affected University Client without undue delay where required.

Provide the University Client with reasonably available information needed to comply with its own statutory notification obligations.

Apply corrective measures where appropriate.

Where personal data is held in a University Client's Platform instance, the University Client is responsible for determining whether notification to affected individuals or regulators is required.

AppliedHE may assist the University Client where required and reasonably practicable, but AppliedHE does not assume the University Client's legal responsibilities as the Organisation under the PDPA.

Nothing in this Policy constitutes an admission of liability by AppliedHE, a warranty of absolute security, or a waiver of any right, defence or limitation of liability available to AppliedHE under applicable law or contract.

10. Retention

AppliedHE retains personal data only for as long as necessary to fulfil the purposes for which it was collected, to provide the Platform, to comply with legal obligations, to resolve disputes, to enforce agreements, or as otherwise permitted by law.

For personal data held in a University Client's Platform instance, the University Client determines the applicable retention period.

Upon termination of a University Client's use of the Platform, AppliedHE will handle Customer Data in accordance with the applicable Terms of Service, Data Protection Statement and any written agreement with the University Client.

AppliedHE may retain backup copies for a limited period where technically necessary, subject to security controls and routine deletion cycles.

For personal data collected directly by AppliedHE through its public website or communications, AppliedHE will retain such data only for as long as reasonably necessary for the purpose collected, unless a longer retention period is required or permitted by law.

11. Your Rights Under the PDPA

Subject to the conditions and exceptions under the PDPA, you may have the following rights:

Right of Access

You may request information about personal data held about you and how it has been used or disclosed.

Right to Correction

You may request correction of personal data that is inaccurate, incomplete, misleading or out of date.

Right to Withdraw Consent

You may withdraw consent for the collection, use or disclosure of your personal data, subject to reasonable notice and any legal or contractual consequences.

Right to Data Portability

Where applicable under the PDPA, you may request that certain data be transmitted to another organisation.

If your personal data is held in your University Client's Platform instance, you should direct your request to your University Client first, as it controls that data.

AppliedHE will provide reasonable assistance to the University Client where required and practicable.

If your personal data is held directly by AppliedHE, such as data submitted through our public website, you may contact AppliedHE's Data Protection Contact using the details in Section 16.

We may take reasonable steps to verify your identity before responding to a request. We will respond within a reasonable period and, where applicable, within the period required by law.

12. Marketing Communications

AppliedHE may send marketing, administrative or service-related communications to University Client representatives, prospective clients or users who have consented to receive such communications, or where otherwise permitted by law.

You may opt out of marketing communications by:

Using the unsubscribe link included in applicable emails.

Updating communication preferences where available.

Contacting us using the details in Section 16.

Service-related or administrative communications, such as account notices, security alerts, platform updates and transactional messages, may still be sent where necessary to operate the Platform.

AppliedHE complies with applicable Do Not Call and anti-spam requirements. We do not knowingly send marketing messages to Singapore telephone numbers registered with the Do Not Call Registry without valid consent or an applicable exemption.

University Clients are responsible for ensuring that their own communications to End Users through the Platform comply with applicable marketing, anti-spam, privacy and data protection laws.

13. Children's Data

The Platform is intended primarily for use by alumni, students and staff of higher education institutions.

AppliedHE does not knowingly collect personal data from children under the age of 13 through its own public website.

If a University Client allows users below the age of 13, or any higher minimum age required by applicable law, to use the Platform, the University Client is responsible for obtaining all necessary parental or guardian consents and complying with applicable laws.

If AppliedHE becomes aware that personal data of a child has been collected directly by AppliedHE without appropriate consent, AppliedHE will take reasonable steps to delete it.

14. Cookies and Similar Technologies

The Platform uses cookies and similar technologies for:

Strictly necessary cookies

To keep users signed in, maintain sessions and support core Platform functionality.

Functional cookies

To remember preferences such as language, display settings or user choices.

Security cookies

To detect misuse, prevent unauthorised access and protect against security risks.

Analytics or performance cookies

Where enabled, to help understand Platform performance and improve user experience. AppliedHE will use aggregated or anonymised information where reasonably possible.

We do not currently use third-party advertising or behavioural tracking cookies through the Platform.

You may control cookies through your browser settings. Disabling strictly necessary cookies may prevent you from signing in or using core Platform features.

15. Third-Party Links and Services

The Platform may contain links to third-party websites, services, payment gateways, job postings, event pages, social media pages or external resources.

AppliedHE is not responsible for the privacy practices, content, security, accuracy, availability or conduct of third-party websites or services.

Where a University Client connects or directs users to third-party services, the University Client is responsible for ensuring that such services are appropriate and compliant with applicable law.

Users should review the privacy policies and terms of any third-party service before using it.

16. Contact Us

If you have questions, requests or concerns about this Privacy Policy or AppliedHE's handling of personal data, please contact:

Data Protection Contact

AppliedHE Pte. Ltd.

7 Temasek Boulevard

#12-07 Suntec Tower One

Singapore 038987

Email: privacy@appliedhe.com

For general enquiries, you may also contact:

AppliedHE Pte. Ltd.

Email: info@appliedhe.com

If your personal data is held in a University Client's Platform instance, please contact your University Client first, as it is responsible for that data.

If you are not satisfied with our response, you may also lodge a complaint with Singapore's Personal Data Protection Commission at https://www.pdpc.gov.sg.

17. Changes to this Policy

AppliedHE may update this Privacy Policy from time to time to reflect changes in law, regulatory guidance, Platform features, business operations, security practices or data handling procedures.

The "Last Updated" date at the top of this Policy indicates when it was last revised.

Where changes are material, AppliedHE will provide reasonable notice, such as by email, website notice, in-app notice or another appropriate method.

Continued use of the Platform after the updated Policy takes effect constitutes acknowledgement of the updated Policy.

18. Governing Law

This Policy is governed by the laws of Singapore.

Any disputes arising from or relating to this Policy shall be subject to the exclusive jurisdiction of the courts of Singapore.

This Policy does not limit any statutory rights that cannot lawfully be excluded or restricted.

19. Relationship with Other Documents

This Privacy Policy should be read together with the ALUMNI-Ready Terms of Service and the Data Protection Statement for University Clients.

If there is any inconsistency between this Policy and a written agreement between AppliedHE and a University Client, the written agreement shall prevail to the extent of the inconsistency, unless otherwise required by applicable law.