ACE INTERNATIONAL BUSINESS SCHOOL

New Baneshwor, Kathmandu, Nepal

DATA PROTECTION POLICY

Personal data of students, applicants and staff

1. Purpose

1.1 Ace International Business School holds personal data relating to the people who study here, the people who apply, and the people it employs. This Policy establishes how that data is collected, used, secured, shared and destroyed, and who is accountable for it.

1.2 The Policy gives effect to the College's obligations under the prevailing law of Nepal and under its agreements with the universities whose programmes it delivers.

2. Scope and Application

2.1 This Policy applies to personal data relating to enrolled students, applicants and enquirers, and all employees, whether full-time, part-time, visiting or on contract.

2.2 It binds everyone who handles that data on behalf of the College, including Board members, management, teaching and administrative staff, IT support, and any contractor or agent given access to College records.

2.3 It applies to data in any form: paper files, records held on College systems, spreadsheets, institutional email, CCTV images, and data held for the College by an external service provider.

3. Definitions

3.1 Personal data means any information from which a living person can be identified, such as a name, address, citizenship or passport number, photograph, student or staff number, marks, attendance, salary or bank details. Sensitive personal data means data concerning health or disability, caste or ethnicity, religion, criminal record, biometric identifiers and financial hardship, and requires additional care. Data subject means the person the data relates to. Processing means anything done with personal data, from collection through to destruction. IT Department means the department holding the data protection function under clause 5.2. Personal data breach means any loss, theft, alteration, destruction or unauthorised disclosure of personal data, whether deliberate or accidental.

4. Data Protection Principles

4.1 Personal data is collected only where it is needed, and the data subject is told why it is being collected.

4.2 It is used only for that purpose. Use for any other purpose requires fresh consent.

4.3 It is kept accurate and corrected when the College is told it is wrong.

4.4 It is kept no longer than the periods set out in Annexure A.

4.5 It is kept secure, by the measures set out in Section 8.

4.6 The College is able to demonstrate, in writing, that it has complied with the above.

4.7 Personal data is normally processed on one of the following grounds: the consent of the data subject; the performance of the enrolment or employment relationship; a legal obligation binding on the College; or the protection of a person's life or safety. Where consent is relied on it must be informed, recorded and capable of being withdrawn.

5. Roles and Responsibilities

5.1 The Board of Directors owns this Policy. The Principal is responsible for its implementation.

5.2 The Information Technology Department holds the data protection function of the College and discharges it in coordination with the Head of the Department that owns the records concerned. The IT Department maintains the register of personal data held by the College, administers access to systems, receives and processes requests and complaints from data subjects, authorises the destruction of records, investigates breaches, arranges the annual briefing, and reports to the Board once a year. The contact details for data protection matters shall be displayed on the notice board and the College website.

5.3 Heads of Department are responsible for the records held in their department. They determine who requires access, keep records accurate, apply the retention periods, confirm before any destruction that the records are no longer required, and notify the IT Department before adopting any new form, system or supplier that will handle personal data.

5.4 Every member of staff is responsible for the data they handle, shall attend the annual briefing, shall comply with Section 8, and shall sign the Confidentiality and Data Protection Undertaking at Annexure B where their role gives access to student or staff records.

5.5 Students collecting personal data for a project or dissertation require the written approval of their supervisor before collection begins.

5.6 Where an external organisation processes personal data for the College, a written agreement is required before any data is transferred, specifying what is shared, for what purpose, for how long, how it will be protected, and that all data will be returned or destroyed when the engagement ends.

6. Transparency and Privacy Notices

6.1 A privacy notice is issued with the admission pack and repeated in the student handbook, and a corresponding notice is issued with the appointment letter for staff. It states what data is collected, why, who it is shared with, how long it is kept, and who to contact.

6.2 Students on the programme of an overseas awarding university are informed in writing that their data is held both by the College in Nepal and by that university abroad, and that the university issues the transcript and certificate.

7. Rights of Data Subjects

7.1 Any student, applicant or member of staff may ask to see their data, request a copy, request a correction, request deletion where the College no longer needs it, withdraw a consent previously given, or make a complaint. Requests are made in writing to the IT Department, which shall verify the identity of the requester and respond within fifteen working days in consultation with the Head of the Department holding the record. Where a request is extensive or complex a further fifteen working days may be taken, and the reason shall be stated.

7.2 No fee is charged for a first request. A reasonable copying charge may be applied to repeated requests.

7.3 A request for deletion shall be refused, with reasons given in writing, where the law requires the record to be retained, where a case or appeal remains open, or where the record forms part of the permanent academic record.

8. Technical and Organisational Security Measures

The following measures apply across the College. Each is capable of being verified by a Head of Department without specialist assistance.

8.1 Technical measures: systems and electronic records

- Every user has an individual login. Passwords are not shared with any person, including IT staff.
- Access to the student records system, the accounts system and personnel files is granted only to staff whose duties require it, on the written approval of the Head of Department, and is withdrawn by the IT Department on the person's last working day.
- Two-step verification is enabled for institutional email and for the student records system wherever the system supports it.
- College computers carry anti-virus protection and automatic updates, and lock automatically when left idle.
- Records are backed up at least weekly, with one copy held off site or with the College's cloud provider. A sample file is restored once a year to confirm the backup is usable, and the result is recorded.
- Files containing lists of student or staff data are password protected before being emailed, with the password sent separately. Group emails use blind copy.
- College data is not held on personal laptops, phones, USB drives, personal email or personal cloud accounts, and is not entered into free online tools, including public artificial intelligence chatbots and translation sites.
- Computers, phones and drives are wiped or physically destroyed before disposal or transfer.

8.2 Physical security measures

- Paper records are held in lockable cabinets in the registry, the HR office and the accounts office. Those rooms are locked outside working hours.
- Files are not left on desks, in meeting rooms, on printers or in vehicles.
- Visitors are signed in and are not left unaccompanied where records are held.
- Records are not removed from the premises without the written approval of the Head of Department.

8.3 Organisational measures

- Staff in admissions, registry, examinations, IT, HR, accounts and academic roles with access to student records sign the Undertaking at Annexure B before access is granted, and sign it again each year.
- Data protection is covered at induction, with one refresher briefing each year. The IT Department maintains the attendance record.
- The IT Department maintains a register showing what personal data the College holds, where it is held, who has access and the applicable retention period. Heads of Department confirm the entries for their own records once a year.
- The exit checklist requires the return of files, keys and access cards, and the closing of accounts, on the last working day.
- The IT Department reviews compliance with this Policy once a year and reports to the Board.

9. Data Sharing and Disclosure

9.1 Personal data is not disclosed outside the College unless the data subject has consented, the law or a court requires it, or the disclosure has already been described in the privacy notice.

9.2 Disclosures already described in the privacy notice include registration and results data sent to the awarding universities, returns to the University Grants Commission and the Ministry of Education, filings with the Inland Revenue Department and the Social Security Fund, and disclosure to auditors and external examiners.

9.3 Data transferred to an awarding university is governed by the data sharing agreement between the College and that university. The IT Department reviews that agreement once a year with the Principal.

9.4 Enquiries about a student from a parent, employer, embassy or agent are not answered without the student's written consent, unless the student is a minor or there is a risk to a person's life.

10. Data Retention

10.1 Retention periods are set out in Annexure A. Where a statute, an awarding university or an auditor requires a longer period, the longer period applies.

10.2 The IT Department maintains a retention register recording, for each category of record, where it is held, which Head of Department is responsible for it, and the date on which it falls due for disposal.

11. Data Deletion and Destruction Procedure

11.1 Annual review. In the first month of each fiscal year, each Head of Department shall list the records in their custody that have passed their retention date and submit the list to the IT Department.

11.2 Hold check. Before any record is destroyed, the Head of Department shall confirm that it is not required for an appeal, a disciplinary case, a legal claim, an audit or an external examiner visit. Any record still required is held back and the reason recorded.

11.3 Authorisation. Destruction proceeds only on the written authorisation of the IT Department, countersigned by the Head of Department.

11.4 Method for paper records. Paper is shredded on College premises in the presence of two members of staff. It is not sold, given away or disposed of with ordinary waste.

11.5 Method for electronic records and media. Records are deleted from the system and from the recycle bin by the IT Department, and pass out of the backups when that backup set is next replaced. Drives and phones being retired are wiped or physically destroyed; reformatting alone is not accepted as deletion.

11.6 Certificate of destruction. Every destruction is entered in a Disposal Register recording what was destroyed, the date, the method, the authorising officer and the names of the two witnesses. The Register is retained for six years.

11.7 Data held by external providers. Where an external organisation has held data for the College, it shall confirm in writing within thirty days of the contract ending that its copies have been deleted.

11.8 Anonymisation. Where a record retains statistical or historical value, the identifying details may be removed instead of destroying the record, provided the data subject can no longer be identified.

12. Data Breach Management

12.1 A lost file, a lost or stolen laptop or phone, an email sent to the wrong recipient, a suspected hacking attempt or any similar incident shall be reported to the IT Department immediately, and in any event within twenty four hours. Nothing is to be deleted in the meantime.

12.2 The IT Department records the incident, contains it, and establishes with the Head of Department concerned what data was involved and who is affected.

12.3 Where data shared with an awarding university is involved, the IT Department shall inform that university's data protection contact within twenty four hours, so that the university can meet its own regulatory deadline.

12.4 Where individuals are likely to be harmed, they shall be informed promptly and in plain language of what has happened and what they should do. Where a criminal offence is suspected, the matter shall be referred to the Nepal Police Cyber Bureau and to the College's legal adviser.

12.5 Within one month of the incident closing, the IT Department shall record the cause and the corrective action taken and report it to the Board. Breach records are retained for six years.

13. Non-Compliance

13.1 Failure to comply with this Policy is a disciplinary matter under the College disciplinary procedure and the Labour Act, 2074. Deliberate misuse or disclosure of personal data may result in dismissal.

14. Complaints

14.1 A complaint concerning the handling of personal data shall be submitted in writing to the IT Department, which shall acknowledge it within five working days and respond within thirty days. If the complainant is not satisfied, the complaint may be escalated to the Principal and thereafter to the Board. Nothing in this Policy prevents a person from seeking a remedy under the prevailing law of Nepal, or, for students registered with an awarding university, from raising the matter with that university.

15. Policy Review

15.1 The IT Department shall review this Policy once a year with the Heads of Department, and sooner if the law changes or if an incident demonstrates that the Policy is not working. Amendments take effect on approval by the Board.

Approval

Approved by the Board of Directors of Ace International Business School.

.....

ace international BUSINESS SCHOOL PVT. LTD.

Name: Dr. Ashish Tiwari
Designation: Executive Director
Date of approval: 17 July 2026
Effective from: 17 July 2026

Annexure A — Data Retention Schedule

Retention periods run from the trigger shown in the third column. Where a statute, an awarding university or an auditor requires a longer period, the longer period applies.

Record	Retention period	Trigger
Core student record: name, programme, dates, modules, results, award	Permanent	Held in the College archive; access limited to the Registrar and the IT Department
Student file: application, certificates, citizenship or passport copy, photographs	7 years	Completion or withdrawal
Applications from candidates not admitted	1 year	Close of the admission cycle
Attendance and internal assessment records	5 years	End of the academic session
Examination scripts and marked coursework	12 months	Publication of results, or the close of any appeal, whichever is later
Student disciplinary files	6 years	Date of the final decision
Counselling, health and disability records	7 years	Last contact; held separately with restricted access
Staff personnel file: contract, qualifications, appraisals, leave	7 years	End of employment
Applications from unsuccessful job candidates	1 year	Date the post is filled
Payroll, provident fund, social security and tax records	7 years	End of the fiscal year (five years is the statutory minimum)
Student fee and other financial records	7 years	End of the fiscal year
Enquiry and marketing contact lists	2 years	Last contact, or immediately on withdrawal of consent
CCTV footage	30 days	Overwritten automatically unless retained for an investigation
Visitor register	1 year	Date of visit
Breach records and Disposal Register	6 years	Closure of the incident or date of destruction

Annexure B — Confidentiality and Data Protection Undertaking

Name	
Designation	
Department	
Employee ID	

My work at Ace International Business School gives me access to personal information about students, applicants and staff, and to information about the College that is not public. In return for that access, I undertake the following.

1. I understand that confidential information includes personal details of students, applicants and employees; marks, examination papers and academic records; disciplinary, counselling, health and financial records; salaries and payroll; and the College's dealings with the universities whose programmes it delivers.
2. I will keep it confidential. I will not pass it to anyone inside or outside the College who does not need it for their work, and I will not discuss it in public, on social media, or with family and friends.
3. I will look at it only when my work requires it. I will not look up records out of curiosity or on someone else's behalf, and I will not copy, photograph or forward records except as my work requires.
4. I have read the AIBS Data Protection Policy and will follow it. In particular I will keep my password to myself, lock my screen when I leave my desk, keep paper files in the cabinets provided, and not take records off the premises without written approval.
5. I will not keep College information on my personal laptop, phone, USB drive, personal email or personal cloud account, and I will not enter it into free online tools, including public AI chatbots.
6. If anything goes wrong, a lost file, a lost or stolen device, an email sent to the wrong person or a suspected hacking attempt, I will inform the IT Department and my Head of Department within twenty four hours.
7. When I leave the College or change role, I will return all records, files, devices, keys and access cards, and delete any College information held on any device approved for my use.
8. This undertaking continues after I leave. My duty of confidentiality over personal information continues without limit of time; over the College's commercial and strategic information it continues for five years.
9. I understand that breaking this undertaking is a disciplinary matter which may lead to dismissal under the College disciplinary procedure and the Labour Act, 2074.
10. This undertaking is governed by the laws of Nepal and the courts of Kathmandu. I will sign it again each year and on any change of role.

I have read and understood the above and I sign it freely.

Employee	For Ace International Business School
.....	.....
Name:	Name and designation:
Date:	Date: