UNITE STUDENTS

Third Party Code of Connection

Version Number:2025/1.0

UNITE STUDENTS

Table of Contents

Click on the section header to be taken straight to the corresponding page.

1 Introduction 3

1.1 Purpose 3

1.2 Scope 3

1.3 Our Commitment & Compliance 4

2 Supplier Information Security Expectations 4

2.1 Core Security Expectations 4

2.2 Incident Notification 4

2.3 Data Protection 5

2.4 Access Management 5

2.5 Subcontracting 5

2.6 Due Diligence & Annual reviews 5

2.7 End-of-Engagement Obligations 6

3 Acknowledgement & Support 6

Appendix A – Document Control Information 7

1 Introduction

1.1 Purpose

This policy outlines the information security expectations for all third-party suppliers who provide services, systems, or handle data on behalf of Unite Students. It is designed to safeguard our customers, uphold our reputation, and maintain trust in our brand.

We are committed to maintaining the **Confidentiality**, **Integrity,** and **Availability** of our data and services. Suppliers play a critical role in our overall security posture, and we expect a high standard of care, professionalism, and alignment with our values in all engagements.

Together, we share responsibility for protecting information and ensuring secure, reliable services. This Code of Connection sets out clear principles to help us achieve that goal collaboratively.

1.2 Scope

This policy applies to all third parties who:

- Access Unite Students systems, networks, or data
- Provide services that involve processing, storing, or transmitting Unite Group/Students information
- Deliver technology, infrastructure, or operational support that integrates with or impacts our business operations
- Provide services or operations that if compromised could negatively impact the trust and reputation of Unite Students/Groups.

This includes, but is not limited to, cloud service providers, software vendors, managed service providers, consultants, and subcontractors.

1.3 Our Commitment & Compliance

At Unite Students, we are committed to protecting the **confidentiality, integrity, and availability** of our data and services. While suppliers are responsible for the security of the services they deliver, we remain ultimately accountable to our customers and stakeholders. We therefore require all suppliers to operate in a way that reflects our values and supports our security objectives.

Compliance with this Code of Connection is mandatory for all suppliers. Failure to meet these requirements, or any serious breach of information security, may result in remedial action, suspension of services, or termination of the contract in line with Unite Students' governance and legal processes.

2 Supplier Information Security Expectations

2.1 Core Security Expectations

Suppliers are expected to take information security seriously and demonstrate a commitment to maintaining robust, fit-for-purpose controls. Security practices should reflect industry best practice and be appropriate to the nature of the service and the sensitivity of the data involved. Suppliers must actively monitor and improve their security posture in response to evolving threats, emerging risks, and changes in technology.

2.2 Incident Notification

Suppliers must notify Unite Students of any actual or suspected information security incident, data breach, or compromise within 24 hours of discovery. Notifications should include:

- A summary of the incident
- Impacted systems or data
- Actions taken or planned
- A point of contact for follow-up

2.3 Data Protection

- All data must be protected against unauthorised access, disclosure, alteration, and destruction.
- Sensitive data should be encrypted with AES-256 both when it is being sent and when it is stored.
- Personal data must be handled in accordance with applicable data protection laws (e.g., GDPR) and any Contract provision or Data Protection Agreement that exists between United Students and the supplier.

2.4 Access Management

- Access to systems and data must be limited to authorised personnel with a legitimate business need.
- Strong authentication mechanisms must be in place, including multi-factor authentication where appropriate.
- Personal email addresses must not be used to access Unite Students' networks, systems, or accounts under any circumstances.

2.5 Subcontracting

- Subcontracting of services involving Unite Students data or systems requires prior written approval.
- Approved subcontractors must adhere to the same security standards and obligations.

2.6 Due Diligence & Annual reviews

- Suppliers requiring access to Unite IT assets must complete a due diligence questionnaire before any access is granted and prior to starting work.
- Where risks or gaps are identified, suppliers are expected to implement recommended improvements or demonstrate clear progress toward mitigation.
- An annual review of the supplier's information security controls will be required to ensure continued suitability and responsiveness to evolving threats.

- Unite Students/Group may also request evidence of security practices or conduct assessments at any time. Suppliers are expected to cooperate fully and transparently.

2.7 End-of-Engagement Obligations

- Upon termination or expiry of the agreement, the supplier must return all Unite Students property (including IT assets) or irretrievably destroy any Unite Students data. Confirmation of completion must be sent in writing to the Procurement team at procurementteam@unitestudents.com within 30 calendar days of termination, unless a shorter period is required by law or contract. Any return must safeguard confidentiality and integrity, for example via tracked delivery by an approved courier or secure handover in person.

3 Acknowledgement & Support

All suppliers must review and formally acknowledge this policy prior to engagement. Ongoing compliance is a condition of continued partnership.

If you have any questions or need guidance, please contact our Information Security team at **informationsecurity@unitestudents.com**. We're here to help you meet these expectations and keep our partnership secure.

UNITE STUDENTS

Appendix A – Document Control Information

Document Management			
Document Ref / Title	Third Party Code of Connection		
Version #	1.0	Status	Live
Classification	Public (everyone has access)		
Reason for development	New Policy		
Summary of changes	New Template		
Applicable parties			
Author(s) (name / title)	Eddie Robinson – Information Security Manager		
Owner (name / title)	Michelle Grist – Head of Information Security & Resilience Eleanor Biddiscombe – Procurement Director		
Function			
Approved by (name/ title)			
Date Approved	23/12/2025		
Review date	01/12/2026		
Location	Bristol		
Distribution	All suppliers		

Consultation			
☐ Data Protection	☐ Communications	☐ NCC / ECC	☐ City Teams
☐ Sales	☐ IT Service Desk	☐ IT	☐ Legal
☐ Finance - AR	☐ Finance - Treasury	☐ InfoSec	☐ HR
☐ Finance - AP	☐ Procurement	☐ H&S	☐ Business Intelligence
☐ Estates	☐ Environment	☐ Marketing	☐ Asset Management
☐ Digital	☐ Office Support	☐ PMO	☐
☐ Commercial Finance	☐ Acquisition / Development	☐ Student Services	☐

Version History (copy and paste from top section to here as a record)			
Version	*Date approved*	*Author*	*Summary of changes*
1.0	23/12/2025	Eddie Robinson	Policy creation

This table is to be used to record all revisions made to this document. Changes made should also be recorded on the Business Management System.