1. Introduction

This document aims to describe the services offered by Zenith School of Studies (referred to as ZSOS in the following sections) to applicants using the company's services for their university application and enrolment. Additionally, it will clarify the terms used in the application and enrolment process, outline ZSOS responsibilities, and address GDPR provisions.

2. Definition of terms

Applicant – Anyone who gets in touch with ZSOS through any available communication channels and expresses interest in applying and enrolling at any of the partner universities.
International applicant – any applicant who needs a visa in order to study in the chosen country.
Home applicant – Any applicant who has permission to live, work, and study in the selected country.
Partner university – Any university that ZSOS has officially partnered with through a signed agreement.
Communication channels can be: The places where you can find information about the company include its website, social media pages (Facebook, Instagram, Twitter), emails associated with the company, and phone numbers for both the office staff and field representatives.
Entry requirements are those specified by each partner university and ZSOS has no influence on any of them.
Admission tests Each partner university sets its own rules for organisation and grading, and ZSOS is not involved in how they are arranged or assessed.
Passing grades each partner university has its own rules; some may use a pass/fail system, while others might employ a grading system ranging from 1 to 10 or 1 to 100.
Application form – the form that needed to be filled in by ZSOS in order to start the application process. Each partner university has its own application form with its own information requirements.
ID – the official identification document that proves the applicant's citizenship.
Diploma/qualification/certificate – any official document that proves the applicant's previous level of qualification.
Residency evidence/visa/student visa – any document that proves the right of the applicant to live, work and study in the country where they choose to study.
Resume – the applicant's resume describing the last 3 years of working experience.
Personal statement - a written description of the applicant's personal details, interests, achievements, and hobbies.
Contact person – any person mentioned by the applicant as a point of contact or reference.
Conditional offer – the offer issued by any of the partner universities describing the conditions that the applicant needs to fulfil in order to be admitted at the respective university.
Unconditional offer – the final offer issued by the partner university offering the applicant their place to study also mentioning the details about the course, duration, tuition fee, mode of study and campus.
UCAS Letter – represents the Confirmation of Acceptance for Studies for international students who need to apply for a student visa.
Finance application – the forms that need to be filled in to obtain finance in the countries where this is available.

3. ZSOS RESPONSIBILITIES

- To reach out to the applicant after they've shown interest in the company's services.
- To provide the most accurate description of the entry requirements for the selected university.
- To make sure the applicant gets the conditional offer letter and help them meet the requirements.
- To schedule the applicant for the entry test where necessary.
- To inform the applicant about the test results. If the applicant doesn't pass and needs to reschedule the test, ZSOS will handle it.
- To inform the applicant when they get the unconditional offer and get the acceptance form signed.

- To guide the applicant with the finance application. ZSOS isn't responsible for decisions made by the partner university or their admission criteria. ZSOS also has no responsibilities over the finance application outcome.

4. GDPR

ZSOS is registered with the Commissioner's Office (ICO). The provision of clause 4 is applicable to all agents and collaborators of ZSOS

4.1 The Principles of Data Protection

ZSOS must comply with the following principles, which are legally enforceable:

- To handle personal and sensitive (about ethnic origin, political opinion, faith, disability, sexual preference, criminal convictions etc.) data fairly and lawfully.
- To be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- To use personal and sensitive data for specified and lawful purposes and shall not be further processed in any manner incompatible with those purposes.
- To use personal and sensitive data, which are reasonable, relevant and not Data Protection Act: V.2 (Reviewed on **28 Sept 2023** Next Review: **Sept 2024**) excessive to that particular purpose.
- Use personal and sensitive data accurately and where necessary, update it
- Keep and protect these personal and sensitive data with an appropriate degree of security.
- Store personal and sensitive data for longer than is necessary for that purpose.
- Any personal and sensitive data would not be transferred outside the UK unless the recipient authorities ensure an adequate level of data protection.
- These personal and sensitive data will be released either with the person's consent or for purpose of the national security.
- Adequate, relevant and not excessive - Data collected must be enough to complete the required task and no more.
- Not kept longer than is necessary - personal information should only be retained by the College for as long as is required to fulfil the purposes for which it was originally provided or required by law to be held. Beyond this point, it should be securely destroyed.

4.2 Data Security

ZSOS and applicants are responsible for ensuring that:

- Any personal data, that they process, is kept securely in accordance with this policy.
- Personal information is not disclosed accidentally or otherwise to any unauthorised third party.

ZSOS should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. Personal information should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, it should be coded, encrypted or password-protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.