

INTO »

UNIVERSITY of
STIRLING



INTO »

UNIVERSITY of
STIRLING



INTO UNIVERSITY OF STIRLING PRIVACY NOTICE

DATE OF ISSUE: October 2021

INTO Stirling LLP

Privacy Notice

INTO Stirling LLP is committed to protecting your privacy. This notice will help you understand how we look after your personal data and how we make sure that we meet our obligations to you under data protection law (referred to in this notice as the "Data Protection Laws").

If you have any questions about this privacy notice or generally how your personal data is processed by us, please contact us by email at: privacy.intostir@intoglobal.com or as specified in the "How To Contact Us" section below.

Introduction

In this privacy notice, the terms "we", "our", and "us" refer to INTO Stirling LLP of registered office address University Of Stirling, Stirling, FK9 4LA (ICO registration number ZA344680).

We are a controller of your information which means that we are responsible for looking after it. We will use your personal data fairly, lawfully and in a transparent manner, and in accordance with the Data Protection Laws.

We give you the power to share in the world of international education as part of our mission to connect you through our innovative partnerships with leading universities, to expand your opportunities for higher education and help you succeed and transform your lives. This notice describes what information we collect from you and how it is used and shared.

Please click on one of the links below to find out more information.

We reserve the right to update this privacy notice at any time by changing it as it applies to your use of our services.

1. [Important information](#)
2. [The information we collect about you](#)
3. [How is your personal information collected?](#)
4. [Basis for using your personal information](#)
5. [How do we use your personal data?](#)
6. [Disclosures of your personal data](#)
7. [Transferring personal data outside the UK](#)
8. [Information security](#)
9. [Information retention](#)
10. [Your legal rights](#)
11. [What happens if I chose not to provide my personal data?](#)
12. [How to contact us](#)

1. Important information

Purpose of this privacy notice

Your trust is very important to us and this privacy notice aims to give you information on how we collect and process your personal data, including any information you may provide when you submit an enquiry, request a brochure, make a direct online application for a course, or when you enter your details onto and use our websites.

It is important that you read this privacy notice together with any other privacy notice or fair processing notice we may provide to you on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your information. This privacy notice supplements the other notices and is not intended to override them.

Please see our further policy if you are an applicant for employment [here](#)

It is important to us that the personal data we hold about you is accurate and current. Please contact us if your personal data which we hold changes during your relationship with us.

If you have any questions about this privacy notice, please contact us by email at: privacy.intostir@intoglobal.com

What do the key terms mean?

"Personal data" means any information which we hold about you from which you can be identified. It may include contact details, identification numbers, other personal information, photographs, expressions of opinion about you or indications as to our intentions about you.

"Processing" means doing anything with the personal data, such as collecting, recording, organising, structuring, storing, adapting or altering, retrieving, accessing, consulting, disclosing, disseminating, aligning or combining, restricting, erasing or destroying or using the data in any way.

Third-party links

Our website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share information about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

2. The information we collect about you

Depending on which services you use, we collect different kinds of information from or about you. We may collect, use, store and transfer different kinds of personal information about you which we have grouped together as follows:

- **Identity Information** includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth, photograph, video recorded image (which may include recordings of lessons or CCTV images) and gender.
- **Contact Information** includes home address, term time address, email address and telephone numbers and emergency contact information including parent/guardian/next of kin information.
- **Education Information** includes your educational history, qualifications, certifications, and English language test scores.
- **Compliance Information** includes details regarding your visa, and your status as a home or international student.

- **Financial Information** includes bank account and payment card details; and information provided by a third party in relation to your funding (for example your sponsor).
- **Transaction Information** includes details about payments to and from you and other details of the services you have purchased from us.
- **Technical Information** includes internet protocol (IP) address, your login information, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our services.
- **Profile Information** includes your username and password, courses selected by you, your interests, preferences, feedback and survey responses.
- **Usage Information** includes information about how you use our websites and services.
- **Marketing and Communications Information** includes your preferences in receiving marketing from us and related third parties and your communication preferences.
- **Special Categories of Personal Information** includes details about your ethnic origin and your health, disabilities or other medical information that you may provide to us. In certain circumstances we may also receive information from you about any criminal convictions you may have. Please see the "Special Category Data" and Criminal "convictions" sections below and our Special Category and Criminal Offence Data Policy [here](#)

3. How is your personal information collected?

We use different methods to collect information from and about you, including through:

- **Information you provide.** You may give us information including your Identity, Contact, Education and Financial Information by filling in application forms, either in hard copy or online, or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:
 - apply for a place on a course or make an enquiry with us;
 - accept a place to study on a course;
 - request marketing material be sent to you;
 - take part in a survey;
 - share information about studies and/or employment options you followed after studying with us; or
 - give us some feedback or get in contact with us.
- **From websites and apps that use our services.** As you interact with our websites, we may automatically collect Technical Information about your equipment, browsing actions and patterns. We collect this personal information by using cookies and other similar technologies. To find out more about the way INTO's websites use cookies and similar technologies please see below .
- **Third parties or publicly available sources.** We may receive personal information about you from various third parties including Technical Information from analytics providers and search information providers; Contact, Financial and Transaction Information from payment providers who administer payments from you on our behalf; Identity, Contact and Education Information from education counsellors that you engage to act on your behalf and/or from universities who we work with; and Compliance Information from regulatory agencies, for example, UK Visas and Immigration and the Office for Students.

4. Basis for using your personal information

We are passionate about ensuring the success, and transforming the lives, of our students. We will use your personal data to help us ensure that we provide, improve and develop our services for you.

We need to have a valid reason to use your personal data. This is called the "lawful basis for processing". Sometimes we might ask your permission for us to do something with your personal data: for example, when you give your consent to allow us to contact you by email about a new service we are providing. At other times, we don't need to ask your explicit permission because we have another lawful basis for processing your personal data, and you might reasonably expect us to use your personal data. For example, in sending an offer letter to you for the course you have applied to study on, we would be performing our part of the contract we have with you.

Collected information may be used in the following ways:

- where we need to **perform the contract** we are about to enter into or have entered into with you in respect of the course you have applied to study on.
- where it is **necessary for our legitimate interests**. We are required to carry out a balancing test of our legitimate interests in processing your personal data against your interests and rights under the Data Protection Laws. We will only process your personal data when your interests and rights do not override those interests. Our legitimate interests include, but are not limited to:
 - informing and formulating our future strategies;
 - ensuring the smooth running of our business;
 - keeping our facilities safe and secure;
 - keeping adequate records;
 - enabling us to engage with you so that we can provide you with services and tell you about new products and services across the wider INTO Group which we think may be of interest;
 - using your feedback to improve our services;
 - collecting and processing payments;
 - for fraud prevention purposes;
 - sharing academic progress reports with a student's sponsor;
 - supporting you with engagement opportunities delivered by our regional office staff;
 - sharing your personal data with online testing services, and remote proctoring services; and
 - sharing your personal data for intra-group administrative transfers.
- where we need to **comply with a legal or regulatory obligation**: for example, in some of the circumstances relating to the prevention of crime, or because we may be required to share your information with certain statutory bodies (see below for further information about whom we may share your information with).

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason, and that reason is compatible with the original purpose. If you wish to get more information on the basis on which we process your personal information you can contact us via: privacy.intostir@intoglobal.com

5. How do we use your personal data?

We use the information we have to deliver and improve the services we offer to you. Examples of the services offered, and how we use your personal data, include the following:

1. to register you as a new customer when you submit an enquiry to study with us in order that we can respond to you as necessary for the performance of a contract with you or in order to take steps at your request prior to entering into a contract;
2. to process your application to study on a particular course with us: from arranging and conducting interviews with you, and completing statutory visa compliance checks, to sending you an offer letter through to processing your acceptance;
3. to assess your eligibility for alternative INTO courses where you do not meet the entry requirements for the course you have applied for with us where such processing is necessary for the purposes of our legitimate interests;
4. to understand your academic progress in order to be able to assess the performance of our academic staff where this is necessary for the purposes of our legitimate interests;
5. to provide you with advice on study options, or respond to questions about courses where such processing is necessary for the performance of a contract with you or for the purpose of our legitimate interests;
6. to provide you (or if you are under 18, your guardian or next of kin) with information about your application with us where such processing is necessary for the performance of a contract with you;
7. to assess and advise you in relation to your financial eligibility and the financial statements you need to provide as necessary for our performance of a contract with you;
8. to manage your access to our virtual learning environments (VLE), and provide a personalised browsing experience when you access and participate in the VLE where the processing is necessary for our performance of a contract with you;
9. to enable us to provide you with online courses, facilitate the accreditation of your participation in those courses, and other online learning initiatives where this is necessary for our performance of a contract with you or for our legitimate interests;
10. to accept and process payments in relation to events, courses, tests and examinations as necessary for our performance of a contract with you;
11. to collect and process any payments you may owe us in accordance with the relevant [student terms and conditions](#) for the course that you have applied to and/or are studying as necessary for the performance of our contract with you;
12. to deliver our services to you and to provide you with information about them, including letting you know about any new offers, sending you notifications about courses and updates, and details of services which may be of interest to you, and to enable us to personalise our communications to you where such processing is necessary for the purposes of our legitimate interests; teaching and events held in the Centre as well as online teaching sessions in which you participate may be recorded and then made available to view by relevant students and relevant staff;
13. to send a text message with important information to the mobile phone number you have given us to use during term time, for example to let you know about a change to the room where your lecture is being held;
14. to continue to engage with you when you have completed your studies as necessary for the purposes of our legitimate interests or where you have provided your consent;

15. to enable us to conduct analysis, historical research, budget forecasting and management planning where such processing is necessary for the purposes of our legitimate interests in the smooth running of our business;
16. to enable you to participate in any surveys or any other promotions we may be running where such processing is necessary for the purposes of our legitimate interests;
17. to administer and protect our business and our websites where such processing is necessary for the purposes of our legitimate interests;
18. to deal with any requests from you regarding your [rights](#) under this notice to enable us to comply with a legal obligation;
19. to deal with any requests from third parties for disclosure of your personal data where such disclosure is to comply with a legal or regulatory obligation.

Automated decision making

Assumptions are made about your interests depending on the information you have supplied to us about yourself, and about the website you were visiting when you did so. For example, if you enquired about a Foundation course with us, we assume you may be interested in other courses with us.

We also assume you speak certain languages based on your nationality or country of residence. If you require any further information regarding any automated decision making, please contact us at: privacy.intostir@intoglobal.com

Marketing

We aim to provide you with choices regarding how we contact you, around the marketing and advertising of our services.

Promotional offers from us:

We may use your Identity, Contact, Technical, Usage and Profile Information to form a view on what we think you may want or need, or what may be of interest to you: for example, in respect of a new promotion that we are running. We conduct surveys and research and analyse the information that we have in order to evaluate and improve existing products and services and develop new products or features.

You will receive marketing communications from us if you have requested information from us or purchased services from us, or if you provided us with your details when making an enquiry to us; and, in each case, you have not opted out of receiving communications from us.

Cookies

We use cookies and similar technologies to provide and support our services. Please read our [Cookies Policy](#) to learn more.

Special Category Data

We may hold information about you which is classified as 'special category data' in the Data Protection Laws, such as details about your ethnicity and racial or ethnic origin, your political opinions, your religious or philosophical beliefs, your health and any disabilities you may have, your sexual identifier or sexual orientation, your genetic or biometric data and data relating to any criminal (or alleged criminal) offences or convictions, which you have supplied to us.

We will only process this special category data in circumstances where it is legally required, for example, where it is necessary for us to meet our obligations in ensuring an appropriate level of care and facilities can be offered to students with a disability; or where we are required to report on equal opportunities monitoring; or to use temperature testing to ensure the safety of our centre in the context of a pandemic.

We set out more detail in relation to this processing in our Special Category and Criminal Offence Data Policy [here](#)

Criminal convictions

We will only use information relating to criminal convictions where we are permitted to do so by the Data Protection Laws and then only in accordance with our Special Category and Criminal Offence Data Policy. The processing of criminal conviction data occurs when it is necessary for us to comply with the law or for another reason where there is a substantial public interest in us doing so, for example, including the processing of any visa application in line with the United Kingdom Visas and Immigration requirements.

Less commonly, we will, if necessary, use information relating to criminal convictions or alleged criminal behaviour where it is necessary in relation to legal claims, where it is necessary to protect your interests, or someone else's interests and you are not capable of giving your consent, or where you have already made the information public.

6. Disclosures of your personal data

We may share your personal information with other INTO Centres. We may also share your personal information with selected external third parties including:

- our University partner with whom you are applying to study once you have completed your course with us or to facilitate joint courses;
- INTO University Partnerships Limited, IUP2 LLP or other INTO group companies as required;
- education counsellors that you have engaged with to act on your behalf;
- a sponsor or employer who is supporting you through your studies;
- external examiners and assessors;
- third party suppliers, service providers and sub-contractors who perform any services for us: for example, providers of student accommodation; payment processing companies who process your payments on our behalf; technology companies whose systems we use; education service providers who provide online proctoring and online testing; or agencies who provide services to carry out marketing campaigns on our behalf;
- analytics and search engine providers that assist us with the improvement and optimisation of our website;
- professional advisers including solicitors, auditors and insurers who provide legal, insurance and other consultancy services;
- third parties with whom we have a duty to disclose, for example, where disclosure is necessary due to a legal process or an enforceable governmental or regulatory request, such as a request from UK Visas and Immigration Authority;
- the Office for Students (OfS), the Office of the Independent Adjudicator, the Higher Education Statistics Agency (HESA) for statistical analysis and other regulatory bodies as required. See [HESA's collection notices](#) for full details;
- relevant Local Authorities to facilitate your registration on the electoral register, if eligible, so you can participate in elections that may occur while you are studying with us;
- emergency services (for example, Ambulance, Police, NHS Trusts etc.) where we are concerned about your safety/wellbeing or consider you to be a risk to yourself or others to ensure appropriate support is available for you;

- our University partner's Students' Union to enable the provision of membership services; and
- third parties to whom we may choose to sell, transfer or merge part of our business to or with. Alternatively, we may seek to acquire other businesses or merge with them.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and require them to process your personal data for specified purposes in accordance with our instructions.

7. Transferring personal data outside the UK

The information we collect from you may be transferred to, and stored at, destinations outside the United Kingdom (UK). It may also be processed by staff operating outside the UK who work for another INTO entity, an external third party or one of our suppliers. Such staff may be involved in advising you as to which course or university you wish to apply to, helping you with your application to us or providing support services as we require. By submitting your personal data to us, you are acknowledging that it could be being transferred, stored or processed in a location outside the UK (known as a "restricted transfer"). Whenever we transfer your personal data out of the UK, we ensure an equivalent level of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We transfer your personal data to countries that have been deemed by the UK government to provide an adequate level of protection for personal data, known as 'adequacy regulations';
- We transfer your personal data to service providers who have agreed to contractual terms which give personal data the same protection it has in the UK; for the time being we continue to use the contractual terms as approved by the European Commission, both for existing restricted transfers and for new restricted transfers.

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the UK. Now that the UK has left the EU, we will ensure that appropriate transfer mechanisms are in place and follow guidance issued by the Information Commissioner's Office (the UK's data protection regulator).

8. Information security

We place great importance on the steps we take, including use of different technologies and physical and organisational measures, to protect your personal information from unauthorised access and against unlawful processing, accidental loss, alteration, disclosure, destruction and damage.

We have in place procedures and technologies to maintain the security of personal data from the point of collection to the point of destruction. We will only transfer personal data to third parties if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

The confidentiality of any password that enables you to access, for example, our virtual learning environment, is your responsibility, whether we have given you the password or you have chosen it yourself. We ask you to please not share your password with anyone. We will not be liable for any unauthorised transactions entered into using your username, personal information and/or password.

9. Information retention

How long will you use my personal data for?

We will retain your personal data for as long as necessary to fulfil the purposes we collected it for, including satisfying any legal, accounting, or reporting requirements: for example, any reporting requirements we have to comply with for UK Visas and Immigration. We may also retain it for a period after this time as may be necessary and relevant to our legitimate operations.

On conclusion of your studies, the Centre will retain certain personal data that forms part of our student records archive. This provides a record of your registration as a student and your achievements whilst

studying with us, to allow us to respond to future requests for information from you, and to report on performance or any other relevant aspect of the Centre's student body.

We consider a number of factors in deciding how long to keep your personal data: the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements (i.e. whether particular laws mean we have to keep certain types of document for a certain length of time).

In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for statistical purposes, in which case we may use this information indefinitely without further notice to you. We may also retain a record of your stated objection to the processing of your personal data, including in respect of an objection to receiving communications, for the sole purpose of ensuring that we can continue to respect your wishes to not contact you further, during the term of your objection.

10. Your legal rights

You have a number of rights in relation to your personal data under Data Protection Laws, including, the right to:

- **Request access to your personal data** (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data that we hold about you and to check that we are lawfully processing it;
- **Request the correction of the personal data that we hold about you.** This enables you to have any incomplete or inaccurate data that we hold about you corrected, although we may need to verify the accuracy of the new personal data that you provide to us;
- **Request erasure of your personal data.** This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your personal data unlawfully or where we are required to erase your personal data to comply with local law. Please note, however, that we may not always be able to comply with your request for erasure for specific legal reasons which will be notified to you, if applicable, when we respond to your request;
- **Object to the processing of your personal data.** Where we are relying on public interest or a legitimate interest (or those of a third party) you have the right to object to the processing of your personal data where there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling public interest or legitimate interest grounds to process your personal data which override your rights and freedoms;
- **Request the restriction of processing of your personal data.** This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your personal data but we need to verify whether we have overriding public interest or legitimate interest grounds to use it;
- **Request the transfer of your personal data to you or to a third party.** We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where the information is used to perform a contract with you; and
- **Withdraw your consent at any time where we are relying on consent to process your personal data.** However, this will not affect the lawfulness of any processing carried out before

you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent. You can ask us to stop sending you marketing messages at any time by following the “unsubscribe” (or similar) links on any marketing message sent to you or by contacting us at any time. Where you opt out of receiving these marketing messages, this will not apply to personal data provided to us as a result of a purchase, product/service experience or other transactions.

If you wish to exercise any of the rights set out above, or require further information about any of those rights, please contact us at: privacy.intostir@intoglobal.com We will need to request specific information from you in order to be able to deal with your request. This is a security measure designed to ensure that your personal data is not disclosed to any person who has no right to receive it. We will confirm the specific information required from you when you contact us. We may also contact you to ask for further information in relation to any request you make in order to speed up our response.

Time limit to respond:

We aim to respond to all legitimate requests as soon as possible and within one calendar month of receipt. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

11. What happens if I choose not to provide my personal data?

Where we need to collect personal data by law, or under the terms of a contract we have with you and you fail to provide that information when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, we may not be able to offer you an opportunity to study with us). In this case, we may have to cancel the contract you have been offered with us or the services you require from us, but we will notify you if this is the case at the time.

12. How to contact us

If you have any questions or comments about this privacy notice, please contact us as indicated below:

Email: privacy.intostir@intoglobal.com

By post: F.A.O. The Centre Director, INTO Stirling LLP, University of Stirling, Stirling, FK9 4LA.

Thank you for taking the time to read our privacy notice.

INTO University of Stirling

APPROPRIATE POLICY DOCUMENT: SPECIAL CATEGORY AND CRIMINAL OFFENCE DATA

1. In the course of our business, we need to process both Special Category ("**SC**") data and Criminal Offence ("**CO**") data. When we undertake such processing we comply with the UK's General Data Protection Regulation (the "**UK GDPR**") and Data Protection Act 2018 (the "**DPA**") as well as any further laws, codes of practice or guidance in relation to processing personal data and privacy which are either enacted or published by a relevant supervisory authority and which are applicable to us from time to time.
2. Specifically, our processing of SC and CO data complies with Articles 9 and 10 of the UK GDPR, Schedule 1 of the DPA, and the data protection principles set out in the UK GDPR. The purpose of this policy document is to explain how our processing of this kind of data is consistent, where applicable, with these articles, conditions and principles, as well as to tell you about the length of time we need to hold such data.
3. **WHAT IS SC DATA?**
 - 3.1 Article 9 of the UK GDPR defines SC data as being personal data which includes or reveals:
 - 3.1.1 Racial or ethnic origin;
 - 3.1.2 Political opinions;
 - 3.1.3 Religious or philosophical beliefs;
 - 3.1.4 Trade union membership;
 - 3.1.5 Genetic data;
 - 3.1.6 Biometric data for the purpose of uniquely identifying a natural person;
 - 3.1.7 Data concerning health; and
 - 3.1.8 Data concerning a natural person's sex life or sexual orientation.
 - 3.2 Article 10 of the UK GDPR covers the processing of personal data which relates to criminal convictions, criminal offences, or related security measures.
 - 3.3 Data protection law says that we can only process SC data if one of the conditions in Article 9(2) UK GDPR and/or in Schedule 1 of the DPA applies. If we process CO data, then this too must be on the basis of one of the Schedule 1 conditions.
 - 3.4 Most of the conditions for processing SC or CO data also require us to have this document in place (an "Appropriate Policy Document") which explains our procedures for compliance, and for the retention and erasure of the data.
4. **DESCRIPTION OF THE DATA WE PROCESS**
 - 4.1 We process special category data about our employees, prospective employees and former employees, including medical data, data in relation to physical or mental health, passport details and details in relation to equal opportunities monitoring. In each case, we process this data because it is necessary for us to fulfil our obligations or exercise our rights as an employer.

4.2 We process CO data about our employees, prospective employees and former employees as a part of our background checks, or where we need to comply with a legal obligation.

4.3 We also process SC and CO data about our students and prospective students including medical data, data in relation to disabilities, physical or mental health, details in relation to equal opportunities monitoring and criminal convictions.

5. SCHEDULE 1 CONDITIONS

5.1 We rely on the following Schedule 1 conditions when we process SC data:

5.2 Part 1, Schedule 1 – Employment, Health and Research etc

5.2.1 **Paragraph 1(1)(a)** employment, social security and social protection.

Processing includes:

- (a) employee health data, and the passport details of prospective employees in accordance with the above condition when we manage recruitment, business travel and in connection with employee familiarisation trips;
- (b) medical data, physical or mental health data and ethnicity data in accordance with the above condition to create and maintain a personnel file;
- (c) health data in accordance with the above condition to determine absences from work in the context of payroll requirements, and for pension administration.

5.3 Part 2, Schedule 1 – Substantial Public Interest Conditions

5.3.1 **Paragraph 6(1) and (2)(a)** statutory, etc. purposes

Processing includes:

- (a) ethnicity data and other SC data in accordance with the above condition where we are required to monitor equality of opportunity;
- (b) student and prospective student disability data in accordance with the above condition to ensure that we can make reasonable adjustments necessary to ensure equality of access to student accommodation;
- (c) student and prospective student ethnicity data in accordance with the above condition in relation to compliance with visa conditions and assessment of the right to study in the UK;
- (d) student data to comply with our regulatory obligations, for example, complying with our Prevent duties;
- (e) student data relating to disability, ethnicity, gender identity, nationality, religion or belief, sexual identifier, and sexual orientation to make returns for statutory reporting.

5.3.2 **Paragraph 8(1)** equality of opportunity or treatment.

5.3.3 **Paragraph 10(1)** preventing or detecting unlawful acts.

- 5.3.4 **Paragraph 18(1)** safeguarding of children and of individuals at risk.
- 5.4 We only process CO data where such processing is consistent with the following purposes in Parts 1 and 2 of Schedule 1:
 - 5.4.1 **Paragraph 1(1)(a)** employment, social security and social protection.
 - (a) criminal conviction data in accordance with the above condition when we recruit employees.
 - 5.4.2 **Paragraph 6(1) and 6(2)(a)** statutory, etc. purposes.
 - (a) criminal conviction data to comply with our obligations under immigration law.
 - 5.4.3 **Paragraph 10(1)** preventing or detecting unlawful acts.

6. PROCEDURES FOR COMPLYING WITH THE PRINCIPLES

- 6.1 The UK GDPR sets out a number of principles in relation to the processing of personal data. These are set out below, together with measures we have taken to ensure that our processing of SC and CO data is in compliance with them.

6.2 Accountability

- 6.2.1 The UK GDPR requires us not only to comply with the data protection principles set out below, but to be able to demonstrate that we comply with them.
- 6.2.2 We have adopted several measures to meet this accountability requirement, including:
 - (a) carrying out annual data protection refresher training for our employees to ensure that data protection is at the heart of our decision making;
 - (b) implementing and maintaining an accurate record of our processing activities;
 - (c) implementing technical and organisational measures to protect the personal data that we process;
 - (d) putting a process in place to ensure that appropriate agreements are in place with organisations with whom we share personal data;
 - (e) ensuring we have appropriate privacy policies in place, and that our processing is consistent with them; and
 - (f) carrying out, where necessary, data privacy impact assessments.

We regularly review our accountability measures and update or amend them when required.

6.3 Principle (a): processing must be lawful, fair and transparent

- 6.3.1 UK GDPR states that processing must be lawful, fair and transparent. For processing to be lawful, it must be specifically consented to by the data subject, or be necessary for one of the reasons set out in Article 6 of the UK GDPR. If the processing relates to SC or CO data, one of the Schedule 1 conditions must also apply.

- 6.3.2 We have identified a lawful basis for our processing, and a further Schedule 1 condition where the processing involves SC or CO data.
- 6.3.3 We set out our lawful bases for our processing (and the further conditions on which we rely) in our privacy notices, in greater detail in our Record of Processing Activities, and in this document. Our privacy notices provide transparent information about our processing.
- 6.3.4 We only process personal data in ways people would reasonably expect and use data privacy impact assessments and legitimate interests assessments to ensure that our processing is fair.
- 6.3.5 We are open and honest when we collect SC or CO data and do not mislead people about how we use it.
- 6.4 **Principle (b): personal data must be collected for specific and legitimate purposes and processed in accordance with those purposes**
 - 6.4.1 Our privacy notice explains the purposes for which we process personal data, and we do not process personal data for purposes other than these.
 - 6.4.2 We process SC data and CO data only where it is necessary for the purposes set out in one of the Schedule 1 conditions.
 - 6.4.3 We do not process personal data for purposes which are incompatible with the purposes for which they were originally collected (unless this is to comply with a legal obligation, or to exercise a function which is set out in law).
- 6.5 **Principle (c): personal data must be adequate, relevant and limited to what is necessary for the stated purposes**
 - 6.5.1 We aim to ensure we have sufficient SC and CO data for the purposes set out in the Schedule 1 conditions above, but do not collect or otherwise process SC or CO data in excess of what we require for these purposes.
 - 6.5.2 If we become aware that personal data is provided to us which is not relevant for our purposes, we will require employees to erase it.
 - 6.5.3 We use national guidance and take external advice to help us determine what information we need to process.
- 6.6 **Principle (d): personal data must be accurate and, where necessary, kept up-to-date**
 - 6.6.1 We have processes in place to check the accuracy of the SC and CO data we hold, and we record the source of such data.
 - 6.6.2 We correct any inaccuracies in the SC and CO data we hold when data subjects exercise their rights under Article 16.
 - 6.6.3 We keep a record of any challenges to the accuracy of the personal data we hold.

6.7 Principle (e): personal data must be retained for no longer than necessary

6.7.1 We are considering how long we need to process the SC and CO data for to enable us to justify the retention period we decide upon.

6.7.2 As part of our personal data retention review, we will implement reviews of the SC and CO data we hold and seek to erase it when it is no longer necessary for the purposes for which it was collected.

6.8 Principle (f): personal data must be kept securely

6.8.1 Encryption and pseudonymisation are used where it is considered appropriate for the level of sensitivity of the SC or CO data that we are processing.

6.8.2 We train our employees in the secure handling of SC and CO data in particular, and personal data in general.

6.8.3 We limit access to personal data to those of our employees, agents, contractors and third parties who have a business need to know the information.

6.8.4 We ensure that organisations that process personal data on our behalf implement technical and organisational measures which are sufficient to ensure the security of the data being processed.

7. RETENTION AND ERASURE

7.1 As set out above, we aim to retain personal data only for as long as necessary to fulfil the purposes we collected it for, including satisfying any legal, accounting, or reporting requirements (for example, to comply with reporting requirements in relation to the Office for Students, or UK Visas and Immigration, or tax reporting requirements to HMRC). We may also retain personal data for a period after this time if it is necessary and relevant for our legitimate operations.

7.2 In some circumstances we may anonymise personal data (so that it can no longer be associated with an individual) for statistical purposes, in which case we may use this information indefinitely.

7.3 Once an employee, worker or contractor leaves the company we will retain or destroy SC or CO data in accordance with applicable laws and regulation.

8. REVIEW DATE

8.1 This Appropriate Policy Document will be reviewed annually.

Date of issue: October 2021