

INTO »



PRIVACY NOTICE FOR CANDIDATES AND PROSPECTIVE EMPLOYEES OF THE INTO COMPANIES AND ASSOCIATED JOINT VENTURES

May 2021

Contents

About this Privacy Notice.....	3
Introduction.....	3
The information we collect about you	4
How your personal information is collected.....	5
How we will use your personal information	5
If you fail to provide personal information	5
Special Category Data.....	5
Information about Criminal Convictions	6
Automated decision-making	6
Data Sharing.....	6
Information Security.....	7
Information Retention	7
Rights of access, correction, erasure and restriction.....	7
Contacting our Data Protection Officer	8
Changes to this Privacy Notice.....	8

About this Privacy Notice

This privacy notice is issued by the following companies which are referred to in this document as “The Companies”.

In the United Kingdom:

- INTO City LLP
- INTO London World Education Centre Ltd
- INTO Manchester Ltd
- INTO MDX Street LLP
- INTO Newcastle University LLP
- INTO Queens LLP
- INTO UEA LLP
- INTO University of Exeter LLP
- INTO University of Stirling LLP
- INTO University Partnerships Ltd
- IUP2 LLP
- Newcastle University INTO London LLP
- Delta Language and Training Consultancy Ltd (trading as NILE)

In the United States of America

- INTO CSU, LLC
- INTO Marshall, LLC
- INTO Mason, LLC
- INTO North America, Inc.
- INTO NY at Drew, LLC
- INTO OSU, Inc.
- INTO SLU, LLC
- INTO Suffolk, LLC
- INTO UAB, LLC
- INTO USF, Inc.
- INTO WSU
- INTO Illinois State University, LLC

Outside the UK and US

- INTO China Ltd (WFOE)
- DPU China
- IUP (Asia) Ltd (Topco)
- IUP Asia Ltd

Each of The Companies and INTO as a global organisation is committed to protecting the privacy and security of your personal information.

Introduction

In this privacy notice, the terms "we", "our", and "us" refer to The Companies listed above.

Each of The Companies is a controller of your personal 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.

This privacy notice describes how we collect and use personal information about you while you are applying to work with us, either as an employee or contractor. This notice does not form part of any contract of employment or other contract to provide services.

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

If you have any questions in relation to this notice or generally about how your personal information is processed, please contact our Data Protection Officer by email at: privacy@intoglobal.com

What do the key terms mean?

"Data Protection Laws" means (a) to the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of individuals with regards to the Processing of Personal Data; and (b) to the extent the EU GDPR applies, the law of the European Union or any member state of the European Union which relates to the protection of individuals with regards to the Processing of Personal Data.

"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. Personal data does not include data where the identity has been removed (anonymous data).

"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.

The information we collect about you

When you apply to work with us, we may collect, store, use and transfer different kinds of personal information about you which we have grouped together as follows:

- **Identity Information** includes first name, previous last name, current last name, username or similar identifier, marital status, title, date of birth, gender, dependants (USA only), and images such as photographs and videos.
- **Contact Information** includes home address, telephone numbers, personal email address, next of kin and emergency contact information.
- **Compliance Information** includes National Insurance / Social Security number, copy of driving licence and passport, and for relevant posts, results of enquiries to the UK Disclosure and Barring service or local equivalent in other countries.
- **Recruitment Information** includes copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process, results of reference requests, statutory eligibility to work verification, and personal information you provide to us or questions you ask us during an interview, whether conducted in person, by telephone or by video conferencing.

We may also carry out processing activities using special category data:

- for the purposes of equal opportunities monitoring and reporting when information about your race, nationality or ethnic origin will be used;
- to make any reasonable adjustments that may be needed during the recruitment process that are requested by the candidate, for example whether adjustments need to be made during a test or interview; e.g. a candidate with accessibility needs;
- to meet our obligations under the Fair Employment and Treatment regulations for candidates based in Northern Ireland.

Most commonly, we will process special categories of personal data when the following applies:

- you have given explicit consent to the processing;
- we must process the data in order to carry out our legal obligations;
- we must process the data for reasons of substantial public interest; or
- you have already made the data public.

How your personal information is collected

We may collect personal information about candidates from the following sources:

- You, the candidate;
- Any recruitment agency appointed by you or us;
- Any appointed background check provider or similar government agency (US only);
- For certain roles and locations, any credit or other referencing agency;
- Criminal records checking service (DBS in the UK) in respect of criminal convictions;
- Reference providers;
- Publicly available information including LinkedIn and other social media sites.

How we will use your personal information

We will use your personal information to:

- Objectively assess your skills, qualifications, and suitability for the role applied for;
- Carry out background and reference checks, where applicable;
- Communicate with you about the recruitment process;
- Keep records related to our recruitment processes;
- Comply with legal or regulatory requirements;
- Perform statistical analysis (although this data will be anonymised).

It is in our legitimate interests to decide whether to appoint you to the role applied for since it would be beneficial to our business to appoint someone to that role and we need to process your personal information to decide whether to make an offer of employment to you.

We will use information about you during the recruitment process to make decisions regarding suitability for shortlist, interviewing, reference checking, offer and appointment.

If you fail to provide personal information

If you fail to provide certain information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application. For example, if we require a check of your criminal records (known as a DBS check in England and Wales; a Disclosure Request in Scotland; or AccessNI in Northern Ireland), a pre-employment credit check or references for a particular role and you fail to provide us with relevant details, we will not be able to take your application further.

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 trade union membership, your health and any disabilities you may have, your sex life 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 you have given your explicit consent, where it is legally required, where it is necessary for us to meet our obligations or exercise our rights as an employer, where there is a substantial public interest in doing so, or where you have already made the data public. We set out more detail in relation to this processing in our [Special Category and Criminal Offence Data Policy](#).

We may also use your special category data in the following ways:

- for the purposes of equal opportunities monitoring and reporting when information about your race, nationality or ethnic origin will be used;
- to make any reasonable adjustments that may be needed during the recruitment process that are requested by the candidate, for example whether adjustments need to be made during a test or interview; e.g. a candidate with accessibility needs;
- to meet our obligations under the Fair Employment and Treatment regulations for candidates based in Northern Ireland;
- to use temperature testing to ensure the safety of our sites in the context of a pandemic

Information about Criminal Convictions

We will only use information relating to criminal convictions where permitted to do so by 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, in relation to safeguarding of students or similar.

Where appropriate, we will use information relating to criminal convictions or alleged criminal behaviour 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.

For certain roles we are required and/or entitled to carry out a criminal records check to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable. In particular:

- We are required by law to carry out criminal record checks for those carrying out teaching and other roles where there may be unaccompanied contact with minors;
- Some roles, for example, senior roles in Finance, Human Resources and Legal require a high degree of trust and integrity and so we may ask you to seek a basic disclosure of your criminal records history.

Automated decision-making

You will not be subject to decisions that will have an impact on your application based solely on automated decision-making.

Automated decision-making typically takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

- Where we have notified you of the decision and given you 21 days to request a reconsideration.
- Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

Data Sharing

We may share your personal information with credit checking, other referencing agencies and recruitment agencies for the purposes of processing your application.

All our third-party service providers and other entities in the INTO Group are required to take appropriate security measures to protect your personal information in line with our policies.

We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

There are some roles where the recruitment process includes employees of our partner universities and INTO Companies other than the one you have applied to. In these cases we will share your personal and relevant sensitive personal information with those specific employees solely for the purposes of the recruitment process.

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 your personal data to third parties if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

Details of these measures may be obtained from our Data Protection Officer via email: privacy@intoglobal.com

Information Retention

We will keep your personal information for a period of twelve months after we have communicated our decision to you about whether to appoint you to the role applied for. We retain your personal information for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy your personal information in accordance with our data retention policy or applicable laws and regulations.

If we wish to retain your personal information on file, on the basis that a further opportunity may arise in future and we may wish to consider you for that, we will write to you separately, seeking your explicit consent to retain your personal information for a fixed period on that basis.

Rights of access, correction, erasure and restriction

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

- **Request access to your personal information** (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it;
- **Request correction of the personal information that we hold about you.** This enables you to have any incomplete or inaccurate information we hold about you corrected;
- **Request erasure of your personal information.** This enables you to ask us to delete or remove personal information 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 information where you have exercised your right to object to processing (see below);
- **Object to processing of your personal information** where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes;
- **Request the restriction of processing of your personal information.** This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it;
- **Request the transfer of your personal information to another 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; and

- **Withdraw your consent at any time where we are relying on consent to process your personal data.** When you applied for a role with one of The Companies, you provided consent for us to process your personal information for the purposes of the recruitment process. You have the right to withdraw your consent for processing for that purpose at any time. To withdraw your consent, please contact our Data Protection Officer, details below. Once we have received notification that you have withdrawn your consent, we will no longer process your application and, subject to our data retention policy, we will dispose of your personal data securely.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact our Data Protection Officer.

Contacting our Data Protection Officer

Email: privacy@intoglobal.com

Address: F.A.O. The Data Protection Officer, INTO University Partnerships Limited, One GloucesterPlace, Brighton, East Sussex, BN1 4AA, England.

Each of The Companies in the United Kingdom are subject to regulation by the UK's Information Commissioner's Office (the "ICO"). You can contact the ICO for advice and support, however, we would really appreciate the opportunity to assist you at the outset if you have any queries regarding this notice or how we use your personal data.

Changes to this Privacy Notice

We reserve the right to update this privacy notice at any time.

If you have any questions about this privacy notice, please contact our Data Protection Officer by email at: privacy@intoglobal.com

DATE OF ISSUE: 30 May 2021