Data Protection Policy
Revision Date: 01.09.2019
OK Student (OK APPLY LTD and VERMILION GROUP LIMITED)

OK Student
9-11 Wollaton Street
Nottingham NG1 5FW
United Kingdom

Vermilion Group works with exceptional individuals, organizations, and businesses with the aim of fast-tracking our students' careers and providing top talent to drive tomorrow's business successes. Email: more@vermiliongroup.org

1. Introduction

OK Student is committed to protecting the privacy and security of personal information which includes the personal data of our staff, customers and other third parties. This Data Protection Policy sets out the minimum standards which must be complied with by the Company.

2. Scope

This Policy sets out how OK Student services (which includes OK APPLY LTD and VERMILION GROUP) ("Company", "we", "our" or "us") identifies and manages its Data Protection responsibilities in accordance with its legal and regulatory obligations.

It is important for staff and customers ("you", "your") to understand the scope of the data protection legislation to enable us to comply with the legislation. This Policy sets out your responsibilities in relation to the data protection legislation, and applies to the entirety of employees, customers and where appropriate third parties working for, or on behalf of OK Student. It is your responsibility to familiarise yourself with this Policy to ensure compliance.

Please be aware that we use secure Customer Relationship Management tools such as ZOHO.eu to process application data. You can view ZOHO's GDPR compliance information online at www.zoho.com/gdpr.html

We also operate as an approved UCAS Centre for applications. You can view UCAS data protection guidelines online at https://www.ucas.com/about-us/policies/terms-and-conditions/data-protection-guidance-advisers

3. Responsibilities

The Board of Directors have overall responsibility to ensure OK Student meets its legal and regulatory responsibilities under GDPR, and to ensure compliance with this Policy. However all staff including University Advisors, Admissions

Officers, Placement Workers and Administration Managers all take responsibility for compliance under their employment.

We use personal data in order to offer professional advisory and application services to our customers. It is important that the way we use (or "process") that personal data is compliant with the GDPR effective immediately.

Employees must contact the UK Director in the following circumstances:
• If unsure of the lawful basis upon which you are processing Personal Data (including the legitimate interests used by OK Student);
• If you believe OK Student's Privacy Notices are incorrect
• If unsure about the retention period for the Personal Data being processed;
• If unsure about what security or other measures necessary to adequately protect Personal Data
• If there has been an actual or suspected Personal Data Breach – Please see the Breach Notification Policy & Procedure;
• If there is a need to transfer Personal Data outside the European Economic Area as this is restricted unless specific legal conditions are met;
• If a request from a data subject to invoke their rights has been received
• Whenever engaging in a significant new, or change in, processing activity which is likely to require a Data Protection Impact Assessment (DPIA) or plan to use Personal Data for purposes other than what it was collected for;
• If planning to undertake any activities involving automated processing including profiling or automated decision-making; and/or
• If wishing to enter into contracts or other activities involving sharing Personal Data with third parties (including our customers and suppliers).

4. The Data Protection Principles

Anyone processing personal data on behalf of the Company must comply with the six principles of GDPR in order to be legally compliant with the Regulation.

Personal data must be:

1. Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);
2. Collected only for specified, explicit and legitimate purposes (Purpose Limitation);
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);
4. Accurate and where necessary kept up to date (Accuracy);
5. Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation); and
6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

5. Lawfulness, Fairness and Transparency

Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

The GDPR only allows Processing for specific purposes. These are known as the lawful grounds of processing or the conditions of processing. You need to comply with one of these grounds to make the Processing lawful and in compliance with the data protection legislation. The most relevant are set out below:

- The Data Subject has given his or her Consent; or
- The Processing is necessary for the performance of a contract with the Data Subject; or
- To meet our legal compliance obligations; or
- To protect the Data Subject's vital interests; or
- To pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

Consent
Consent needs to be a clear indication of agreement either by a statement or positive action to the Processing by the Data Subject. Consent requires affirmative action. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters. Data Subjects must be easily able to withdraw their Consent to Processing at any time. Any withdrawal must be promptly acted upon. Consent may need to be refreshed on a regular basis.

OK Student needs to evidence any Consent that it relies on and retain a record of all Consents so that we can demonstrate that we have obtained the right Consent for the right processing activities.

Transparency
The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes or from customers, we must provide the Data Subject with all the information required by the GDPR.

When Personal Data is collected indirectly (for example, from a third party or publically available source), we must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the Personal Data. We must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which considers our

proposed Processing of that Personal Data i.e. that the individual knew that their Personal Data was going to be passed to us and for what purposed.

This means that all the third parties that we work with who Process Personal Data collected by OK Student should also comply with the GDPR.

6. Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

We cannot use Personal Data for new, different or incompatible purposes from those disclosed to the Data Subject when it was first obtained.

This means if we collect Personal Data for one purpose, we shouldn't then use it for another purpose unless we tell the Data Subject what we are going to do and we have a legal ground to undertake that Processing.

7. Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

We may only collect Personal Data that you require for the services rendered and duties: we do not collect excessive data. We may only Process Personal Data when performing our services requires it. We cannot Process Personal Data for any reason unrelated to service rendered. We should ensure any Personal Data collected is adequate and relevant for the intended purposes. We shouldn't be collecting any field of Personal Data that is not necessary to the reason we are collecting it.

Staff must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with our data retention guidelines. It is also important that any records are destroyed and/ or deleted in accordance with our Data Retention Schedule, as safe and secure destruction is also required to comply with the data protection legislation.

8. Accuracy

Personal Data must be accurate and, where necessary, kept up-to-date. It must be corrected or deleted without delay when inaccurate.

OK Student must ensure that the Personal Data we use and hold is accurate, complete, kept up- to-date and relevant to the purpose for which we collected it. We must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. OK Student must take all reasonable steps to

destroy or amend inaccurate or out-of-date Personal Data.

9. Storage limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

OK Student must not keep Personal Data in a form where the Data Subject could be identified for longer than needed for the purpose or purposes for which we originally collected it (including for the purpose of satisfying any legal, accounting or reporting requirements).

We will maintain the Data Retention Schedule to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with our Data Retention Policy.

OK Student must ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice or Fair Processing Notice.

10. Security Integrity and Confidentiality Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

Employees are responsible for helping OK Student protect the Personal Data we hold. They must comply with security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Category Personal Data from loss and unauthorised access, use or disclosure. You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction.

If you are transferring Personal Data to a third party, or if you want to transfer Personal Data to a third party, and you are in any doubt as to whether there is a lawful basis or appropriate contract in place, you should speak to the UK Director before transferring the Personal Data.

Employees must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

• Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it. This means if you have access to Personal Data but it is not part of your job or role to access or Process such Personal Data, you should not do so.
• Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
• Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes. This means that you should not access or use any Personal Data if you are not permitted to.

Employees must comply with, and not attempt to circumvent, the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

11. Reporting a Personal Data Breach

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable Regulator and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects and/or any applicable regulator where we are legally required to do so. If you know or suspect that a Personal Data Breach has occurred, immediately notify the point of contact for Personal Data Breaches at info@okstudent.co.uk

12. Data Sharing: International Transfers

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

All application data collected by OK Student is processed at the Vermilion Group Admissions Centre based in Lisbon, Portugal, within the EEA.

OK Student may only transfer Personal Data outside the EEA if one of the following conditions applies:
• Appropriate safeguards are in place, such as: binding corporate rules (BCR); standard contractual clauses approved by the European Commission; an approved code of conduct; or a certification mechanism applies; or
• The Data Subject has provided Consent to the proposed transfer after being informed of any potential risks; or
• The transfer is necessary for one of the other reasons set out in the GDPR, including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

13. Data Subject's rights and requests

Data Subjects have rights when it comes to how we handle their Personal Data.

These include rights to:

• Withdraw Consent to Processing at any time;
• Receive certain information about the Data Controller's Processing activities;
• Request access to their Personal Data that we hold;
• Prevent our use of their Personal Data for direct marketing purposes;
• Ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
• Restrict Processing in specific circumstances;
• Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
• Request a copy of an agreement under which Personal Data is transferred outside of the EEA;
• Prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
• Be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
• Make a complaint to the supervisory authority; and
• In limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

All requests should be sent to info@okstudent.co.uk with the Subject Line 'GDPR Request'.

14. Direct marketing

A Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls).

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly acted upon. If a student, alumni member or other Data Subject opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

15. Accountability and Data Protection Impact Assessment (DPIA)

The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

This means that we must have adequate resources and controls in place to ensure and to document GDPR compliance including:
• Appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;
• Implementing Privacy by Design when Processing Personal Data and completing
• DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
• Integrating data protection into internal documents including this Data Protection
• Policy, Privacy Notices or Fair Processing Notices;
• Regularly training on the GDPR, this Data Protection Policy, and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. We must maintain a record of training attendance by OK Student staff; and
• Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles.

16. Changes to this Data Protection Policy

We reserve the right to change this Data Protection Policy at any time so please check back regularly to obtain the latest copy of this Data Protection Policy. We will notify you when we update this Policy.