Data Processing Agreement

The UK GDPR imposes a legal obligation on data controllers and data processors to formalise their working relationship. Aside from the legal requirements, this makes practical and commercial sense.

By having a contract in place with the required terms, controllers and processors are:

- ensuring they each comply with the UK GDPR;
- protecting the personal data of customers, staff and others; and
- ensuring both parties are clear about their role regarding the personal data that is being processed and are able to demonstrate this.

This Data Processing Agreement amends and forms part of the Terms and Conditions (https://emile-education.com/legal/terms/) between Webskape Ltd (“Webskape”) and the customer (“Customer”).

1. Definitions

1.1. In this DPA:

a) “Controller”, “Data Subject”, “Personal Data”, “Personal Data Breach”, “Processing”, “Processor”, and “Supervisory Authority” have the meaning given to them in the GDPR;

b) “Customer Personal Data” means any Customer data that constitutes Personal Data, the Processing of which is subject to Data Protection Law, for which Customer or Customer’s customers are the Controller, and which is Processed by Webskape to provide the Services;

c) “Data Protection Law” means the UK General Data Protection Regulation (“GDPR”) and Privacy and Electronic Communications Regulations (PECR), and their national implementations in the European Economic Area (“EEA”), Switzerland and the United Kingdom, each as applicable, and as may be amended or replaced from time to time;

d) “Data Subject Rights” means Data Subjects’ rights to information, access, rectification, erasure, restriction, portability, objection, and not to be subject to automated individual decision making in accordance with Data Protection Law;

e) “International Data Transfer” means any transfer of Customer Personal Data from the EEA, Switzerland or the United Kingdom to an international organization or to a country outside of the EEA, Switzerland and the United Kingdom;

f) “Services” means the services provided by Webskape to Customer under the Agreement;

g) “Subprocessor” means a Processor engaged by Webskape to Process Customer Personal Data;

and

h) “Standard Contractual Clauses” means the clauses annexed to EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ L 39, 12.2.2010, p. 5-18) as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ L 344, 17.12.2016, p. 100) in conjunction with the UK International Data Transfer Addendum ('UK Addendum').

2. Scope and applicability

2.1. This DPA applies to Processing of Customer Personal Data by Webskape to provide the Services.

2.2. The subject matter, nature and purpose of the Processing, and the types of Customer Personal Data are set out in Appendix 1.

2.3. Customer is a Controller and appoints Webskape as a Processor on behalf of Customer. Customer is responsible for compliance with the requirements of Data Protection Law applicable to Controllers.

2.4. Customer acknowledges that Webskape may Process Personal Data relating to the operation, support, or use of the Services for its own business purposes, such as billing, account management, data analysis, benchmarking, technical support, product development, and compliance with law. Webskape is the Controller for such Processing and will Process such data in accordance with Data Protection Law.

3. Instructions

3.1. Webskape will Process Customer Personal Data to provide the Services and in accordance with Customer's documented instructions.

3.2. Customer may reasonably issue additional instructions as necessary to comply with Data Protection Law. Webskape may charge a reasonable fee to comply with any additional instructions.

3.3. Unless prohibited by applicable law, Webskape will inform Customer if Webskape is subject to a legal obligation that requires Webskape to Process Customer Personal Data in contravention of Customer's documented instructions.

4. Personnel

4.1. Webskape will ensure that all personnel authorized to Process Customer Personal Data are subject to an obligation of confidentiality.

5. Security and Personal Data Breaches

5.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of persons, Webskape will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the measures listed in Appendix 2.

5.2. Customer acknowledges that the security measures in Appendix 2 are appropriate in relation to the risks associated with Customer's intended Processing, and will notify Webskape prior to any intended Processing for which Webskape's security measures may not be appropriate.

5.3. Webskape will notify Customer without undue delay after becoming aware of a Personal Data Breach involving Customer Personal Data. If Webskape's notification is delayed, it will be accompanied by reasons for the delay.

6. Subprocessing

6.1. Customer hereby authorizes Webskape to engage Subprocessors. A list of Webskape's current Subprocessors is included in Appendix 3.

6.2. Webskape will enter into a written agreement with Subprocessors which imposes the same obligations as required by Data Protection Law.

7. Assistance

7.1. Taking into account the nature of the Processing, and the information available to Webskape, Webskape will assist the Customer, including, as appropriate, by implementing technical and organizational measures, with the fulfilment of Customer's own obligations under Data Protection Law to: comply with requests to exercise Data Subject Rights; conduct data protection impact assessments, and prior consultations with Supervisory Authorities; and notify a Personal Data Breach.

7.2. Webskape will maintain records of Processing of Customer Personal Data in accordance with Data Protection Law.

7.3. Webskape may charge a reasonable fee for assistance under this Section. If Webskape is at fault, Webskape and Customer shall each bear their own costs related to assistance.

8. Audit

8.1. Upon reasonable request, Webskape must make available to Customer all information necessary to demonstrate compliance with the obligations of this DPA and allow for and contribute to audits, including inspections, by the Customer and performed by an independent auditor as agreed upon by Customer and Webskape.

8.2. Webskape will inform Customer if Webskape believes that Customer's instruction under Section 8.1 infringes Data Protection Law. Webskape may suspend the audit or inspection, or withhold requested information until Webskape has modified or confirmed the lawfulness of the instructions in writing.

8.3. Webskape and Customer each bear their own costs related to an audit.

9. International Data Transfers

9.1. Webskape shall gain explicit consent if required to perform International Data Transfers to any country.

10. Notifications

10.1. Customer will send all notifications, requests and instructions under this DPA to Webskape's Data Protection Manager via email to Privacy@Webskape.com. Webskape will send all notifications under this DPA to Customer's registered email address.

11. Liability

11.1. Subject to any limitation of liability set out in the Agreement, to the extent permitted by applicable law, where Webskape has paid damages or fines, Webskape is entitled to claim back from Customer that part of the compensation, damages or fines, corresponding to Customer's part of responsibility for the damages or fines.

12. Termination and return or deletion

12.1. This DPA is terminated upon the termination of the Agreement.

12.2. Customer may request return of Customer Personal Data up to ninety (90) days after termination of the Agreement.

13. Modification of this DPA

13.1. This DPA may only be modified by a written amendment by Webskape with notice given to the Customer.

14. Invalidity and severability

14.1. If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

15. Jurisdiction

This DPA is governed by the laws of the UK and subject exclusively to the courts of the UK.

APPENDIX 1 - PROCESSING

1. Data Subjects

The Customer Personal Data Processed concern the following Data:

- Customers - School name, address and phone number
- Students - Student names, class name, school year, usernames, UPNs, and indications of ability of a student including the time and duration of all visits to our websites, users' scores in exercises, and the time taken to achieve those scores; and
- School staff – Staff names, their email addresses and contact details

2. Sensitive data

The Services are not intended to Process special categories of data.

3. Processing operations

The Customer Personal Data will be processed to provide the Services to the Customer.

APPENDIX 2 - SECURITY MEASURES

Webskape will implement the following types of security measures:

1. Physical access control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Customer Personal Data are Processed, include:

- Establishing security areas, restriction of access paths;
- Establishing access authorisations for employees and third parties;
- Access control system (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Door locking (electric door openers etc.);
- Security staff, janitors;
- Surveillance facilities, video/CCTV monitor, alarm system; and
- Securing decentralized data processing equipment and personal computers.

2. Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g. password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Creation of one master record per user, user-master data procedures per data processing environment; and
- Encryption of archived data media.

3. Data access control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Customer Personal Data in accordance with their access rights, and that Customer Personal Data cannot be read, copied, modified or deleted without authorisation, include:

- Internal policies and procedures;
- Control authorisation schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access Customer Personal Data without authorisation;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure;
- Encryption of data at rest using platform encryption via AWS; and
- Encryption of data in motion using SSL certificate encryption.

4. Disclosure control

Technical and organizational measures to ensure that Customer Personal Data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Customer Personal Data are disclosed, include:

- Encryption/tunneling;
- Logging; and
- Transport security.

5. Entry control

Technical and organizational measures to monitor whether Customer Personal Data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

- Logging and reporting systems; and
- Audit trails and documentation.

6. Control of instructions

Technical and organizational measures to ensure that Customer Personal Data are Processed solely in accordance with the instructions of the Controller include:

- Unambiguous wording of the contract;
- Formal commissioning (request form); and
- Criteria for selecting the Processor.

7. Availability control

Technical and organizational measures to ensure that Customer Personal Data are protected against accidental destruction or loss (physical/logical) include:

- Backup procedures;
- Mirroring of hard disks (e.g. RAID technology);
- Uninterruptible power supply (UPS);
- Remote storage;
- Anti-virus/firewall systems; and
- Disaster recovery plan.

8. Separation control

Technical and organizational measures to ensure that Customer Personal Data collected for different purposes can be Processed separately include:

- Separation of databases;
- “Internal client” concept / limitation of use;
- Segregation of functions (production/testing); and
- Procedures for storage, amendment, deletion, transmission of data for different purposes.

APPENDIX 3 - SUBPROCESSORS

We do not sell or share your data without your consent, other than those subprocessors we use for our business operations under our control. The subprocessors we use are:

- Amazon Web Servers - hosting services https://d1.awsstatic.com/legal/aws-dpa/aws-dpa.pdf;
- Cloudways - hosting services - https://www.cloudways.com/wp-content/uploads/2018/06/cloudways_dpa.pdf ;
- Microsoft – office & email systems https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA ;
- Google – office & email systems - https://cloud.google.com/terms/data-processing-addendum ;
- MailJet – email marketing campaigns - https://www.mailjet.com/legal/dpa/ ;
- Xero – accounting systems - https://www.xero.com/uk/legal/terms/data-processing/