Learning Management System - Privacy Policy

We recognize that visitors to our Learning Management System (LMS) may be concerned about what happens to information they provide when they make use of the system.

We also recognize that education and training establishments have a duty of care to protect the privacy of information provided by their students and employees when they make use of the LMS.

This privacy policy outlines the obligations and requirements of LJ Create and of the education and training establishments that make use of the LMS.

By using the LMS users agree to the terms and conditions outlined in this policy.

1 Definitions

For the purpose of this policy, the following words and expressions shall have the following meanings:

Policy This privacy policy.

Data Controller The legal person or any other body which alone or jointly with others determines the purposes and means of the Processing of Personal Data. For the purpose of this Policy the Data Controller is the education or training establishment making use of the Service.

Data Processor The natural or legal person, authority, agency or any other body which processes Personal Data on behalf of the Data Controller and in accordance with the terms of this Policy. For the purpose of this Policy the Data Processor is LJ Create.

Data Protection Legislation All applicable legislation and regulations relating to the protection of the fundamental rights and freedom of natural persons and, in particular their right to privacy with respect to the processing of Personal Data applicable in the country in which the Data Controller is established.

Data Processing Systems All the software, hardware and systems used by the Data Processor to process the Personal Data and to fulfil its obligations under this Policy.

Data Subject Any student or employee of the Data Controller.

Data Protection Authority The authority responsible for the enforcement of the applicable Data Protection Legislation.

Personal Data Any information relating to a Data Subject.

Processing Includes both automatic processing and manual processing, provided that in respect of manual processing the manual data is organized in a relevant filing system (as defined under the Data Protection Legislation) and “Processed” shall be construed accordingly.

Spam Regulations All applicable laws, rules and regulations regarding the sending of unsolicited electronic commercial messages.

Services The provision of the LMS product by the Data Processor.

2 Services and Personal Data

2.1 The LMS is a cloud-based learning environment provided by LJ Create to its educational and training establishment customers.

2.2 LJ Create provide customers with a set of login credentials for pre-generated system accounts.

2.3 LJ Create licenses the use of learning materials to customers based on the products they have purchased.

2.4 Customers can make use of the LMS to provide educational material to their employees and students.

2.5 Customers can enable their employees and students to access the LMS individually by creating user accounts. When creating a user account an initial set of data is required which includes a username, first name, last name, email address and password. Customers can choose whether to use real names or aliases for this data. Customers can enable employees and students to self-register on the LMS.

2.6 Customers can assign learning content to user accounts to meet their particular requirements. This can be achieved by allocation of user accounts to groups. As this happens employee and student group membership and assigned work is stored within the LMS.

2.7 Customers are required to ensure that system account credentials are kept secure.

2.8 As students work through the learning content, their results are tracked and stored within the LMS.

2.9 Employees have the ability to generate reports based on student data.

2.10 Students can print their performance data reports for personal retention and control.

2.11 Students can edit their own password.

2.12 Students can request that their teacher or administrator edit their user details including first name, last name, email address and password.

2.13 Employees can edit or delete student user personal details.

2.14 Employees can delete student result data.

2.15 Customers are required to ensure that any Personal Data that is extracted from the LMS by its employees is safeguarded.

2.16 LJ Create operates an archiving system to retain student and employee data for a period of no more than 7 years.

2.17 LJ Create retains the right to share aggregated de-identified student data for the development, promotion and improvement of its Services.

2.18 Employee and student data stored within the LMS is and will remain the property of the customer.

2.19 Under no circumstances will LJ Create act as or become the Data Controller of the Personal Data. The customer is and will stay the sole Data Controller of the Personal Data.

2.20 Access to student data requires a site code along with either; a student username and password, or an employee username and password.

2.21 Individuals can request a copy of all data relating to them stored within the LMS. This request should be made to the individual's LMS site administrator. The LMS provides the site administrator with the ability to generate data for an individual in a tab-separated file that can be opened in popular spreadsheet software and text editors.

2.22 Individuals can request that data held about them, within the LMS, is rectified. This request should be made to the individual's LMS site administrator. The LMS provides the site administrator with the ability to rectify data for an individual.

2.23 Individuals can request that all data relating to them, within the LMS, is permanently deleted. This request should be made to the LMS site administrator. The LMS provides the site administrator the ability to permanently delete all data for an individual.

2.24 Individuals that have an LMS account have the right to complain to the Information Commissioner's Office if they believe there is a problem with the way their data is being handled.

2.25 The LMS website makes use of TLS (Transport Layer Security) to guarantee the integrity of the web pages and to ensure customer data is transported securely through an encrypted (SHA-256) point-to-point tunnel between browser and server.

3 Obligations of the Data Processor

3.1 The Data Processor agrees and warrants that it will:

(a) only process the Personal Data in accordance with the terms and conditions set out in this Policy and in accordance with any further written instructions from the Data Controller;

(b) unless otherwise agreed in writing, only process the Personal Data to the extent and in such manner as is necessary for the provision of the Services or as is required by law or any regulatory body;

(c) keep the processed data strictly confidential and ensure that each of its employees, agents and/or permitted subcontractors engaged in processing the Personal Data will be informed of the confidential nature of the Personal Data;

(d) implement appropriate technical and organizational measures to protect Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. Such measures shall be appropriate to the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage to Personal Data and to the nature of Personal Data to be protected;

(e) promptly notify the Data Controller if it receives a request from a Data Subject to have access to Personal Data or any other complaint or request relating to the Data Controller's obligations under the Data Protection Legislation and provide full cooperation and assistance to the Data Controller at the Data Controller's sole cost and expense in relation to any such complaint or request (including, without limitation, by allowing Data Subjects to have access to their Personal Data);

(f) comply with all reasonable requests or directions by the Data Controller to enable the Data Controller to verify and/or procure that the Data Processor is in full compliance with its obligations under this Policy;

(g) provide the Data Controller with full details of any complaint or allegation that the Data Controller is not complying with the Data Protection Legislation by a Data Subject or from the relevant Data Protection Authority;

(h) assist the Data Controller (at the cost of the Data Controller) in taking any action that the Data Controller reasonably deems appropriate to deal with such complaint or allegation pursuant to clause 3.1 (a).

3.2 Notwithstanding anything else in the Policy, the Data Processor shall not be in breach of the Policy to the extent that any such breach and/or failure to comply with the Policy is necessary to comply with the Data Protection Legislation and/or any rule, order or enforcement notice of a competent authority in respect of the Data Protection Legislation.

3.3 Upon the termination of the provision of the Service all Personal Data processed by Data Processor on behalf of the Data Controller and its copies will be immediately returned/provided to the Data Controller, or the Data Processor shall, by the choice of the Data Controller, destroy all Personal Data and certify the Data Controller that it did so.

4 Obligations of the Data Controller

4.1 The Data Controller agrees and warrants that it shall:

(a) provide the Data Processor with clear, comprehensible and specific written instructions with regard to the Processing of Personal Data by the Data Processor for any activity required beyond that of the normal Services;

(b) provide the Data Processor with specific written instructions with regard to the security and confidentiality of the Personal Data in accordance with applicable Data Protection Legislation for any activity required beyond that of the normal Services;

(c) inform the Data Processor of any legitimate inspection or audit of its Processing of Personal Data by any competent Data Protection Authority which relates to the Processing by the Data Processor;

(d) provide the Data Processor with prior notice of any intended inspection of the Processing of Personal Data under this Policy;

(e) inform the Data Processor immediately of any access request, request for correction or blocking of Personal Data or any objection made by a Data Subject related to the Processing of Personal Data by the Data Processor;

(f) comply with all relevant provisions of the Data Protection Legislation and Spam Regulations, including but not limited to the following general obligations:

- the informing of Data Subjects regarding the processing of their Personal Data through a privacy statement or other appropriate means;
- the notification of the processing of Personal Data to the Data Protection Authority;

- the compliance with applicable Spam Regulations regarding the sending of unsolicited messages, either electronically or by ordinary post.

5 Indemnity

5.1 The Data Controller shall indemnify the Data Processor against each claim, loss, liability and cost incurred by the Data Processor as a result of unlawful Data Processing by the Data Controller, the breach of any relevant legislation, including but not limited to relevant Data Protection Legislation and Spam Regulations or the breach of this Policy by the Data Controller or any of its employees, agents or sub-contractors.

5.2 The Data Controller shall inform the Data Processor immediately regarding any claim or any threat thereof that is made to the Data Processor in relation to this Policy.

5.3 The Data Processor shall indemnify the Data Controller against each claim, loss, liability and cost incurred by the Data Controller as a result of a material breach of the obligations of Data Processor under this Policy.

5.4 The Data Processor shall inform the Data Controller immediately regarding any claim or any threat thereof that is made to the Data Controller in relation to this Policy.

6 Supported Regional Privacy Policies

6.1 The Data Processor adheres to the regional privacy policies as listed in document P9240 (LMS – Supported Regional Privacy Policies).

Revision History

Revision	Date	Change
A		Original
B	20 Jul 2016	Various changes
C	5 Jun 2017	Added section for support of regional privacy policies.
D	12 Mar 2018	Added sections required by GDPR: Section 2.21 (data subject's right to access and receive digital copy of data) added. Section 2.22 (data subject's right to rectify data) added. Section 2.23 (data subject's right to erase data) added. Section 2.24 (data subject's right to complain) added.
E	26 Sep 2018	Added section 2.25 declaring transport layer security.