Customer agreement for the use of itslearning Plagiarism

The Licensee has ordered access to the itslearning Plagiarism Control. Plagiarism Control includes SimCheck, a service supplied by Turnitin, LLC with itslearning acting as a reseller.
In connection with the provision of the Plagiarism Control service, and integrated services, the parties agree the following:

1. itslearning facilitates the technical integration of the itslearning Plagiarism Control and Turnitin´s SimCheck through its assignment tool. Turnitin provides the actual plagiarism check service and reports it´s finding back to the itslearning platform that makes it available to its users.

2. The Licensee understands that use of Plagiarism Control involves personal data being transferred from itslearning to Turnitin. A separate Data Processing Agreement must be signed between the Licensee and Turnitin. (See attachment 1)

3. The Licensee can use itslearning´s standard support services for questions, issues or errors related to the Plagiarism Service. But itslearning's responsibility for Turnitin´s SimCheck service is limited to forwarding such requests to Turnitin. itslearning is not responsible for the level of quality of the service that is provided by Turnitin.

4. The Licensee understands that any deficiencies in SimCheck due to matters outside the itslearning application are not the responsibility of itslearning. This means itslearning is not liable for losses that errors, or deficiencies cause at the Customer.

5. If plagiarism or other abuse is suspected such that it is necessary for the Licensee to include itslearning in the activity beyond that available in the standard itslearning interface, itslearning may invoice the Licensee for actual hours used according to applicable standard rates.

6. Likewise, itslearning´s Standard Service Subscription Agreement, or any Master Agreement signed between licensee and itslearning, also apply in relation to this agreement.

DATA PROCESSING AGREEMENT

v.03.09.2020

This Data Processor Agreement (**"DPA"**) is entered into as of …… 2020 between:

Turnitin LLC, 2101 Webster Street, Suite 1800, Oakland CA 94612 USA (the **"Processor"**); and

[Institution name and address] (the **"Controller"**);

who may be referred to as a **"Party"** or the **"Parties"** as the context so requires.

RECITALS

Whereas:

- Controller needs to have Personal Data processed by Processor for the purpose of the performance of the Agreement;
- the general provisions from this DPA apply for all processing of Personal Data in the performance of the Agreement, and in the event of a conflict between those terms, this DPA shall apply;

DEFINITIONS

"AGREEMENT" shall mean either the Processor's Registration Agreement previously entered into by the Parties or an alternative agreement entered into by the Parties in relation to the provision of Processor's services to the Controller;
"GDPR" shall mean the General Data Protection Regulation (Regulaton (EU) 2016/679 of the European Parliament and of the Council);
"Personal Data" shall have the meaning defined in the GDPR;
"Processing" shall have the meaning defined in the GDPR.

Any terms not otherwise defined herein, shall have the meaning specified in the Agreement.
The Parties agree as follows:

1. General

1.1 The Processor undertakes to process Personal Data on the terms and conditions of this DPA on the instructions of the Controller. The Processor shall process the Personal Data lawfully, with due care and in accordance with the GDPR.

1.2 The Processor shall only effect Processing to the extent necessary to provide its services to the Controller as described in the Agreement.

1.3 Only employees who need access to Personal Data to contribute to the operation of the services will have such access to that Personal Data.

1.4 Subject to instructions received from the Controller, the Processor shall not retain Personal Data made available to it in the context of the Agreement any longer than is necessary (i) for the performance of the Agreement; or (ii) to comply with any of its statutory obligations.

1.5 The Processor shall only process the Personal Data on and in accordance with the instructions of the Controller. The Processor will not process the Personal Data for its own benefit, for the benefit of third parties (other than when the Institution has selected standard database repository settings), and/or for its own

purposes or advertising purposes or other purposes, notwithstanding any of its obligations to the contrary under mandatory law.

1.6 The Processor is obligated to promptly inform the Controller regarding any changes in the performance of the Agreement affecting its obligations hereunder, so that the Controller can monitor its compliance.

2. Use of Third-Party Suppliers

2.1 Only third-parties necessary in the provision of the Services may process Personal Data for the strictly limited purposes of providing the services to the Controller. The Controller provides its general written consent to the use of third-party suppliers in the provision of the services. In the event that a new third-party is engaged by Processor from 25 May 2018, Processor shall notify the Controller to give them the opportunity to object to the engagmemet of that third-party.

2.2 In the event the Processor engages third-party suppliers for the provision of the services, the Processor warrants it has a written agreement with the relevant third-party supplier which shall include the mandatory provisions of Article 28(3) GDPR. From 25 May 2018, such third-parties may only be engaged by Turnitin if they are GDPR compliant.

2.3 The Processor indemnifies the Controller from and against all claims by third-parties asserted against the Controller due to a breach of the obligations under this DPA regarding the processing of Personal Data that is attributable to the Processor or third-party suppliers engaged by the Processor.

3. Security

3.1 Processor shall have in place appropriate technical and organisational measures pursuant to Article 32 GDPR with regard to data security, including appropriate data centre security measures. Such non-exhaustive measures are described in Annex A.

3.2 On request, the Processor shall promptly provide to the Controller written information relating to the security of Personal Data.

4. Obligation to report data breaches

4.1 In the event of a: (i) loss of Personal Data, or (ii) breach of the security measures described in Annex A resulting in compromise of Personal Data; the Processor shall notify the Controller promptly after the incident was first discovered. The Processor shall take all commercially reasonable measures to prevent or limit unauthorised and unlawful processing, without prejudice to any right the Controller might have to other measures.

4.2 In the event of a breach, the Processor shall provide to the Controller all relevant an necessary information relating to the breach. The Processor warrants that the information provided will be complete and correct.

4.3 At the Controller's request, the Processor shall cooperate appropriately in informing the competent authorities.

5. Audit

5.1 The Processor warrants that it undergoes periodic third-party penetration testing of its network (at least annually), and utilizes the resulting reports to make changes to its Services as it deems necessary.

5.2 The Processor shall submit to and comply with commercially reasonable audits by Controller during the Term. If it is established during such an audit that the Processor has failed to comply with the provisions of the

Agreement and the DPA, the Processor shall take all commercially reasonable measures to remediate such failure.

6. Data Transfer

6.1 Data Transfers on the Amazon Web Services (AWS) Platform:

6.1.1 The AWS platform stores 100% of submitted content on a localized data centre in the EU (currently in Frankfurt, Germany). Randomized and encrypted sections of such submissions are processed in the USA for comparison purposes. It is not possible to re-compile submissions in the USA from the data that is processed in the USA.

6.2 Data Transfers on non-AWS Platforms:

6.2.2 Non-AWS services are provided exclusively from USA based data centres located in Sacramento and Santa Clara, California.

6.3 Regardless of whether a Service is based on the AWS platform or not, Personal Data will only be transmitted and stored in encrypted form, using proprietary and secure encryption technology on a SOC2 certified infrastructure.

6.4 The Processor warrants that any processing of Personal Data in connection with the performance of the Agreement performed by or for the Processor, including the third-parties engaged by it, will (when transferred outside the EEA) take place only within the USA. Processor will adhere to the EU Standard Contractual Clauses on data transfer incorporated at Annex B.

7. Investigation Requests

7.1 If the Processor receives a request or order from a supervisory authority, government agency or investigation, prosecution or national security agency to provide (access to) Personal Data, the Processor shall immediately notify the Controller. When handling the request or order, the Processor shall observe all of the Controller's lawful instructions (including the instruction to leave the handling of the request or order in full or in part to the Controller) and provide appropriate cooperation.

8. Informing Data Subjects

8.1 The Processor shall cooperate appropriately so that the Controller can comply with its legal obligations in the event that a Data Subject exercises its rights under GDPR concerning the processing of Personal Data.

8.2 If a Data Subject, in relation to the execution of its applicable rights, contacts the Processor directly, the Processor shall not substantively respond unless expressly instructed otherwise by the Controller, but shall immediately report this to the Controller, with a request for further instructions.

8.3 If, in the context of the Agreement, the Processor offers the Service directly to end users whose Personal Data are processed, the Processor is required to inform the end user about the following in an easily accessible and permanently available manner:

a. the name and address of the Processor;
b. the purposes for which the Processor processes the Personal Data;
c. the Personal Data categories processed by the Processor;
d. the countries to which the Personal Data are transferred;
e. the right to access, correct and delete the Personal Data.

The Processor shall notify the Controller where this information is published.

9. Article 28(3) GDPR Compliance

9.1 The following applies to the processing by the Processor:

Subject matter of the processing*:*	Processing of submissions (student or academic papers, examination answers or proposed published texts) and their associated personal data pursuant to the purpose described below.
Duration of the processing*:*	Indefinitely unless instructed in writing by the Controller to delete the Personal Data. The Processor retaining Personal Data (submission content only) allows its Services to improve annually by adding to the database of content against which comparisons are made.
Nature of the processing*:*	Textual comparison services, storage, use, database compilation, grading.
Purpose of the processing*:*	To allow the Processor's customers (academic institutions / publishers) to detect potential plagiarism in the academic / publishing sectors, and to allow the streamlining of grading.
Type of personal data*:*	Generally names, email addresses, student IDs, submission content, examination answers.
Categories of Data Subjects*:*	Students, account administrators, instructors, authors.
Obligations of the Controller:	The Data Controller is obliged to comply with its general obligations under the GDPR, in particular to process the personal data it collects in accordance with Articles 5 and 6, and to comply with Articles 13, 14, 24, 30 and 32, and to comply with any actionable rights of the data subject.
Rights of the Controller*:*	The Controller may exercise its rights against the Data Processor under the GDPR, in particular under Articles 28 and 32.

9.2 The Processor confirms that it:

(a) processes the Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32 GDPR;

(d) respects the conditions in paragraphs 2 and 4 of Art.28 GDPR with regard to engaging other processors;

(e) taking into account the nature of the processing, assists the Controller by utilising appropriate technical and organisational data protection measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;

(f) assists the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the Controller, deletes or returns all the Personal Data to the Controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the Personal Data; and

(h) makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

9.3 Where the Processor engages another processor for carrying out specific processing activities on behalf of the Controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 of Art.28 GDPR shall be imposed on that other processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of that other processor's obligations.

10. Changes

10.1 If either Party makes a material change to the Personal Data to be processed or to the processing, the parties shall consult on amending the arrangements made in this DPA.

10.2 Such changes can never have the effect that the Parties cannot comply with applicable laws and regulations relating to Personal Data.

11. Term and Termination

11.1 The term of the DPA is equal to the term of the Agreement or the duration of processing, whichever is longer. The DPA cannot be terminated separately from the Agreement.

11.2 In the event of written request from the Controller during the Term or upon termination of the Agreement, the Processor shall delete and destroy Personal Data and certify such destruction in writing.

12. Governing Law and Dispute Resolution

12.1 Performance of this DPA shall be governed by the laws of [INSERT MEMBER STATE OF EU CUSTOMER].

12.2 Any dispute between the Parties which cannot be amicably settled without recourse to the courts in connection with the DPA shall be submitted to the competent court in [INSERT].

Signed for and on behalf of **Processor**

……

Print name:

Signed for and on behalf of **Controller**

……

Print name:

ANNEX A: TECHNICAL & ORGANISATIONAL MEASURES

GDPR Technical & Organisational Measures v23.07.2020

1 Introduction

Turnitin, as a part of its services, collects and maintains data to fulfil its contractual obligations to Controller. To accomplish this, Turnitin has created a set of standard operating procedures and measures that enable secure, reliable operation of the Turnitin services.

2 Technical Measures

Pursuant to Article 32 GDPR, Turnitin utilises the following technical measures to ensure data security:

2.1 Turnitin's services are designed with security and high availability in mind. Turnitin's services operate across several thousand servers and thousands of disk drives, using load balancers, custom software, and other techniques to automatically distribute load and maintain redundant copies of data at all times.

2.2 Turnitin currently operates its customer-facing services out of two primary data centers in Sacramento and Santa Clara, California, USA. Turnitin also makes use of AWS regions for data localization.

2.3 Turnitin may also operate equipment in other smaller datacenters in the United States or European Union for networking and data redundancy reasons. Each datacenter has N+1 redundancy for power and cooling systems, and access is limited to Turnitin's staff and approved contractors who need access to perform their work duties. Turnitin's private corporate network provides secure, encrypted, and redundant connectivity between Turnitin's offices and its data centers.

2.4 SOC2 compliance was awarded to our technical infrastructure in May 2018 and proof of certification can be provided upon request. Turnitin is continuously audited for SOC compliance.

2.5 Turnitin is Cyber Essentials certified. Our certification can be viewed at: https://www.cyberessentials.ncsc.gov.uk/cert-search/?query=turnitin

2.6 Other technical measures include:

- Intrusion detection systems;
- File integrity monitors;
- Network security scanners;
- Security event monitoring;
- Sophisticated firewalls;
- All data is encrypted in flight using up-to-date HTTPS encryption. This includes encryption from the client web browser to the load balancer / firewalls, internally between servers and on the WAN between datacenters. Encryption utilises a proprietary, one-way hash method providing pseudonymisation;
- All data is encrypted at rest.
- Encryption applies to Personal Data that is written into databases that reside in encrypted filesystems (AES-256 cipher), which are backed up continuously (files replicated in N+3 redundancy), the back-ups of which are encrypted in a separate server farm. All data is written into a one-way proprietary encryption format;

- SSL network security including Qualys ™ grades of 'A' applicable to all relevant domains used in the solution;
- Employee device encryption and central management;
- Periodic third-party penetration testing of Turnitin's network.

2.7 Databases are backed up continuously. Submissions are replicated five times - 4 on active storage and 1 copy on a back-up server.

2.8 Storage devices are encrypted in accordance with the US Federal Information Processing Standards (FIPS) Publication 140-2.

2.9 Turnitin's infrastructure is compliant with the 'SANS Top 20' security controls as published by the Center for Internet Security Critical Security Controls for Effective Cyber Defense.

2.10 Equipment removed for off-site maintenance is sanitized of any Personal Data in accordance with NIST SP 800-88 Revision 1. We sanitize or destroy media containing Personal Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for re-use.

3 Organisational Measures

3.1 Turnitin has appointed a Data Protection Officer voluntarily who can be contacted at DPO@turnitin.com and has appointed a Chief Information Security Officer to assist the Data Protection Officer with their role and to continuously monitor Turnitin's data security practices.

3.2 Turnitin has instigated an ongoing programme of GDPR awareness training within its organisation and receives Executive level support for data protection initiatives.

3.3 Turnitin has adopted the following non-exhaustive policies in relation to GDPR compliance to assist the Controller with its obligations:

- Data Breach Notification Policy;
- Data Protection Policy;
- Data Retention Policy;
- Data Subject Access Request Policy;
- and Privacy Policy available at: https://help.turnitin.com/Privacy_and_Security/Privacy_and_Security.htm

3.4 Access to machines that contain Personal Data is restricted to only specific, security-trained personnel who may only access these systems in their normal, day-to-day work activities. All access and privilege escalation is monitored and logged for 2 years. Remote access is only possible using cryptographic SSH keys, and physical access is restricted to authorized employees via badge access - all server racks have locked cage doors with codes that are only known to Turnitin employees.

3.5 Turnitin's technical infrastructure is continuously audited by AICPA.

3.6 Turnitin's on-call technology team provides 24/7 coverage for our services by monitoring and alerting on any issues or problems with servers, operating systems, network devices (switches/routers)

backup systems. and server-side performance. Turnitin will notify the customer immediately of any changes to its environment that could adversely impact security.

3.7 Turnitin continuously monitors the National Vulnerability Database and patches as necessary.

ANNEX B: STANDARD EU MODEL CLAUSES

The Standard Contractual Clauses for the transfer of personal data to processors outside the European Economic Area (New Processor Clause), last updated February 2010, are hereby incorporated into this Agreement by reference, amended as follows:

Amendments to Standard Contractual Clauses for the Transfer of Personal Data

Data Exporter shall mean the Controller.

Data Importer shall mean the Processor.

With reference to clause 9 of the Standard Contractual Clauses for the transfer of personal data to processors established in third countries, the Governing Law is the law of [INSERT MEMBER STATE OF EU CUSTOMER]

With reference to Appendix 1:

The Data Exporter is:

The academic institution using the services of the Data Importer as described immediately below.

The Data Importer is:

A provider of services to the academic and private sectors, to assess academic submissions/texts for originality. Clients use the service as a form of plagiarism prevention, and also to streamline grading.

The Personal Data transferred concern the following categories of data subjects:

Individual authors and users of the services.
Individuals who wish to receive commercial information.

The personal data transferred fall within the following categories of data:

Name, title, email address, institution name - all required.
Mailing address, phone number - optional.

The personal data transferred fall within the following categories of sensitive personal data:

Not applicable unless sensitive Personal Data is contained within a submission's content, in which case it is processed lawfully under Art.9 GDPR.

The personal data transferred will be subject to the following basic processing activities:

Creation and maintenance of user profile, responses to service queries, comparison checks.

With reference to Appendix 2:

Refer to Annex A of the DPA.

Signed for and on behalf of **Processor**

……

Print name:

Signed for and on behalf of **Controller**

……

Print name: