DATA PROTECTION AND SECURITY POLICY

Hot Rocks Consulting for PeerAssessment.Com
Last Updated: June, 13 2021

Definitions

Vendor ***(Processor)***	Hot Rocks Consulting LLC The Vendor is responsible for processing data using PeerAssessment.Com on behalf of the Controller. HRC manages logical system design and all financial aspects of the System, conducts troubleshooting for end users, provides user training and instructions, maintains the website.
Responsible Person	Robert Anson Dr. Anson is the owner and founder of Hot Rocks Consulting
Developer	Thrive Web Designs, LLC. Thrive is responsible for all development, upgrade, maintenance of the System on behalf of the Vendor.
Staff	We will refer to 'Staff' as all employees, contractors or volunteers associated with the Vendor and Developer who participate on activities related to PeerAssessment.Com.
GDPR	Means the General Data Protection Regulation
System	Means the PeerAssessment.Com, an application for collecting, storing and reporting student team peer assessment information. This application is owned by Hot Rocks Consulting and was developed by Thrive Web Design.
Institution ***(Controller)***	The institution is a school or college that manages instructors and students, setting rules for their conduct. They are, with instructors, a joint controller directing and managing how personal data is processed. They actively coordinate class operations and policies, manage student and instructor data and policies, set policies and practices, plus oversee contracts regarding third party systems. The institution, in most cases, possess one or more email domains with which email address accounts are assigned to individuals. They provide data to instructors about students in their classes to organize and manage the class and activities.
Instructor ***(Controller)***	In addition to teaching students in a class, they decide on using teams and peer assessments. Their role is 'Controller' (in GDPR terms) because they determine why and how personal data should be processed. Their second role is 'Data Subject', in that the System stores and processes data about them. The Instructor decides to use PeerAssessment.Com and why, load Student data, set timing, select questions, set expectations, and calculate grades. We will include

	with the Instructor any individuals who assist the instructor with peer assessments. For this document, Instructor will also include the role of 'Program Administrator'. Usually this is an Instructor. The Program Administrator is a person who may purchase a 'program' of additional classes for use by themself or other instructors They are able to create, access and edit any classes purchased with the program and monitor who is using the program.
Student	The student is a primary data subject in that most personal data in the System is about them. This is a person who enrolled in a class taught by one or more instructors. The student will enter their feedback regarding themselves, their team, and teammates into the system. Also, they will receive reports of feedback entered by their teammates in which the author of the feedback is anonymous.

A. Statement and purpose of policy

1. Hot Rocks Consulting LLC (the **Vendor**) is committed to ensuring that all personal data handled by us and our developer will be processed according to legally compliant standards of data protection and data security related to the GDPR.
2. We confirm for the purposes of the data protection laws, that the Vendor is a data processor for a limited range of personal data regarding Students and Instructors in connection with their institutional activities. This means that we determine the purposes for which personal data is processed, and the way it is processed.
3. The purpose of this policy is to help us achieve our data protection and data security aims by:
    a. Notifying Instructors and Students about the types of personal information we may hold about them and what we do with that information;
    b. Setting out the rules on data protection and the legal conditions that must be satisfied when we collect, receive, handle, process, transfer, and store personal data and ensuring staff understand our rules and the legal standards; and
    c. Clarifying responsibilities and duties in respect of data protection and data security.
4. General provisions:
    a. This policy applies to all personal data processed by the Vendor.
    b. This policy shall be reviewed at least annually.

B. GDPR Data protection principles

1. The Vendor is committed to processing data in accordance with its responsibilities under the GDPR.
2. Article 5 of the GDPR requires that personal data shall be:
    a. **Lawfulness, fairness and transparency** -- processed lawfully, fairly and in a transparent manner in relation to individuals;
    b. **Purpose limitation** -- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving

purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c. **Data minimization** -- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. **Accuracy** -- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. **Storage limitation** -- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f. **Integrity and confidentiality (security)**-- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures."

g. **Accountability** -- The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

C. Who is responsible for data protection and data security?

1. Maintaining appropriate standards of data protection and data security is a collective task shared between us (Staff) and you (Users). This policy, and the rules contained in it, apply to all Staff, which includes everyone associated with the Vendor and Developer who participate on system-related activities.

    a. The Responsible Person shall take responsibility and accept accountability for the Vendor's ongoing compliance with this policy.

    b. Questions about this policy, or requests for further information, should be directed to the Responsible Person.

    c. All Staff have responsibility to comply with this policy, to handle all personal data consistently with the principles set out here, and to ensure that measures are taken to protect the data security. The Responsible Person must be notified if this policy has not been followed, or if it is suspected this policy has not been followed, as soon as reasonably practicable.

    d. Any breach of this policy will be taken seriously and may result in disciplinary action up to and including dismissal. Significant or deliberate breaches, such as accessing Instructor or Student personal data without authorization or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

2. Users (Instructors and Students) similarly must assume responsibility for protecting and securing data they have access to via reports, download files and System and screen access. It is everyone's responsibility to make sure that printed data they can access is properly secured or disposed of, that electronic data is secured or deleted, and that they properly log in and out of the System.

D. Why we process your personal data?

1. This section describes the reasons for processing your personal data, how we use such information, and the legal basis for processing. We will not process your personal information for any other reason
2. The overarching reason we process personal data is to support teaching and learning in collaborative educational environments. Specifically, there are four reasons that we collect, process, and store your peer assessment data:
    a. To provide feedback to individual Students to facilitate improving their team skills;
    b. To provide feedback to Student teams to facilitate improving their team processes;
    c. To provide feedback to Instructors to facilitate their efforts to help Students collaborate more positively and productively; and
    d. To support researchers to better understand how student teams—and teams in general—work and learn together. Some important outcomes include scholarship of teaching and learning to study collaborative pedagogical approaches, plus efforts to measure the effectiveness of academic programs (e.g. accreditation). All data released for research purposes has erased all personal identifiers; none of the research will involve identified individuals.
3. We commit to the following practices with respect to your personal data:
    a. We will never sell or give your personal information to any third party who seeks to use it for any reason beyond providing or supporting your access to, or use of, Peerassessment.com or conducting research;
    b. We will use your contact information only to communicate with you for purposes directly related to your use of, Peerassessment.com–providing assistance, requesting needed information, or improving the site or services; and
    c. We will collect and store only the absolute minimum amount of personal information for the minimum length of time which is necessary for your effective access to, or use of, the system.

E. What types of personal data and activities are covered by this policy?

1. This policy covers personal data:
    a. which relates to natural living Instructors and Students;
    b. which is stored electronically in the System as raw data or reports rendered into HTML, PDF, CSV or EXCEL formats OR exists in electronic/non-electronic forms in the hands of Staff, Instructors and Students;
    c. in the form of statements of opinion or judgment as well as facts;
    d. which we obtain, is provided to us, which we hold or store, organize, disclose or transfer, amend, retrieve, use, handle, process, transport or destroy.
2. This personal data is subject to legal safeguards set out in the data protection laws.

F. How do we collect this personal data?

1. We collect Student personal data in two ways:
    a. the Instructor loads Student personal data from a file or enters it into the System while preparing for team peer assessment activities within a class; and
    b. Students enter information about themselves, their team, or their teammates in response to questions selected by the Instructor.
2. We collect personal data about Instructors which is:
    a. provided by the Instructor when registering a personal account on the System; or
    b. entered by the Instructor when creating a class on the System.

G. What personal data is processed by PeerAssessment.Com?

1. The Vendor promises to protect your 'personal data' that it stores and processes. 'Personal data' includes any data related to an identified or identifiable natural person, known here as the data subjects. Direct identification can occur using specific pieces of data called identifiers, while indirect identification combines some stored data with other data (which you may or may not possess) to distinguish one specific person. Related personal data is referring to other information that, while it may involve or have some bearing on individual data subjects, it cannot reasonably be used to distinguish one subject from another.
2. In terms of the System, these personal data concepts are described below:
    a. **Data Subjects –** All data subjects-- Students and Instructors--are System users. (Program Administrators are grouped with Instructors, for this document, as they both involve the same personal data). No other subjects are represented in any way by data stored in the System.
    b. **Identifiers –** All data subjects are randomly assigned a UserID in the System. This is used to join any information related to that data subject. A unique UserID is assigned to each data subject. However, other personally identifying information is required to associate the random UserID value to an identifiable natural person.
        i. the principle data identifiers used to distinguish individual Students and Instructors in the system include, Email and Name (last and first);
        ii. if the Instructor chooses to include it, Students may also have a StudentID issued by their institution;
        iii. Instructors may include a Phone number.
    c. **Related Personal Data –** The range of data stored in the system, that is related to the data subjects, can be categorized as follows:
        i. **Academic Location –** This data includes the institution, term, class (which connects the instructor and student), and team (which connects a set of students). This data does not constitute a Student identifier because it can not point to a single Student. However, term and class can be used to reasonably identify an Instructor.
        ii. **Assessment –** A class may include many assessments in which Students can be assessed as members of the same teams or of different teams. The assessment connects Students

together with one another, and with the evaluation they supply or receive. An assessment includes sets of questions that Students can respond to during data collection, and email messages with links to enable Students to enter the survey.

iii. **Response Data** – When Students are assessed, they are responding to prompts about themselves and their Student teammate peers. Each response is identified by the responder UserID, and the target UserID (or left blank if the response target is the overall team or other.)

iv. **Purchase Data** – Information about program and class purchases is stored in the System. This information includes the institution, institutional purchasing address, the number and type of credits purchased, together with plan and program names and codes which can be given to instructors to use the credits to create classes for use. No credit card information is entered, or stored, in our System.

H. What is the level of risk to your personal data?

1. Some of the processing that the Vendor carries out may result in risks to privacy.
2. Should processing result in a high risk to data subject rights and freedoms, the Vendor will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.
3. At this time, the level of risk to personal data is believed to not be "high" based on the following considerations:
    a. the System is built upon technologies that are well tested and widely used for app development;
    b. neither location nor behavior of data subjects is systematically tracked or monitored;
    c. there is no systematic monitoring of publicly accessible places;
    d. no sensitive personal data is processed, related to "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation";
    e. no automated decisions are made about people with legal or significant effects;
    f. the System is designed for use in higher education settings where Students are predominantly of adult age, and rarely 16 or under. Where Students are 16 or under, it is the responsibility of the Controller to ensure that proper consent is established;
    g. there are no reasonable expectations that physical harm could result to the data subjects should a leak occur.

I. How do we limit the risks of storing personal data?

1. Minimizing the personal identifiers and sensitive information is a key first step in limiting the risks of personal data being stolen by third party actors.
    a. As noted, there are only a few pieces of data that could potentially identify an individual person.

b. Also, there is no sensitive personal information collected or stored on the site.

2. The second step is equally important—to limit the amount of time we store personally identifying data.

   a. The System only stores Student identifiers while they are absolutely needed--when students are actively engaged in a peer assessed class. The identifiers are used for student communications and reporting.

   b. When the class ends, or a Student withdraws from the class, we automatically erase Student identifiers.

      i. The related personal data, with no personal identifiers, remains in the System keyed by UserID and a pseudonym (created by hashing the email address). This protects the personal data privacy should a data breach occur.

      ii. The related personal data remains in the system for two reasons. First, if a Student takes another peer assessed class, the new instructor will load a new set of Student identifiers into the System. The pseudonym can be used to establish fresh connections between their new and historical data. Second, the data can be used in research with the identifiers stripped away.

   c. We store Instructor identifiers while the Instructor potentially needs them to log into the System, to create new classes, and access information from completed classes.

      i. For Instructors, these identifiers make up their account used to log in to the System. The account must remain available to the Instructor regardless of whether an institutional site license is still active or whether there are purchased credits remaining to create classes. Instructor accounts must remain active in case the institutional license restarts, or new credits are purchased.

      ii. Instructor identifiers are necessary for communications and reporting purposes; but in addition, the instructor can access their peer assessment history. The Instructor can log in to access past class assessment reports (with now anonymized student data), and to copy forward set-up parameters (related to classes, assessments, questions, messages) to build new classes.

   d. Instructor identifiers will be erased when the Instructor requests to be removed from the System.

      i. When the identifiers are erased, the related personal data remains in the System keyed by UserID and a pseudonym (created by hashing the email address). This protects the personal data privacy of the Instructor should a data breach occur.

      ii. At this point the Instructor will no longer be able to log into PA.

      iii. The Instructor may ask the Processor to create a new account for them based on the same email address. Their history can be restored using the pseudonym to establish fresh connections between their new and historical data.

J. How do we keep your data secure?

Data Security

1. We will use appropriate technical and organizational measures to keep personal data secure, confidential, available, and to protect against unauthorized or unlawful processing, accidental loss, destruction or damage.
2. Maintaining data security means making sure that:
    a. only people who are authorized to use the information can access it;
    b. where possible, personal data is pseudonymized or encrypted;
    c. information is accurate and suitable for the purpose for which it is processed; and
    d. authorized persons can access information if they need it for authorized purposes.
3. By law, we must use procedures and technology to secure personal information throughout the period that we hold or control it, from obtaining to destroying the information. These approaches include:
    a. limiting access through various means;
    b. pseudonymization and encryption of personal data;
    c. secure data transport through SSL certificates and encrypted form posting;
    d. using cloud-based, resilient, high availability servers to maintain processing systems and services;
    e. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
    f. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
4. Personal information must not be transferred to any person or process (eg while performing services for us on or our behalf), unless that person has either agreed to comply with our data security procedures or we are satisfied that other adequate measures exist.
5. Key security procedures include:
    a. personal data will not be regularly printed or stored outside of the protected database;
    b. if personal data is required to troubleshoot issues, any electronic or printed versions of the data will be deleted/destroyed immediately after the issue is resolved;
    c. computers should be locked with a strong password that is changed regularly or shut down when they are left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to other;
    d. no data, at any time, will be stored on CDs or memory sticks;
    e. data should never be saved directly to mobile devices such as laptops, tablets or smartphones;
    f. all servers containing personal data must be approved and protected by security software;
    g. servers containing personal data must be kept in a secure cloud location behind firewalls and

malware protection.

6. The processor will be able to restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process that includes at least daily backups.
7. The processor will assess the appropriate level of security, taking into account the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.
8. We ensure that Sub-processors we use also implement appropriate technical and organizational measures.
9. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller.

Storage and Retention

10. Student personal data will only be stored within the System where it is protected by the security measures in place, except for temporary periods needed to troubleshoot issues.
11. We will only hold your personally identifying data on the Systems while the Student is actively engaged in a class that is using the System, or until the data subject requests that their identifying data be removed.
12. Automatic backups will be run once daily and retained for at least one week.

Data Breaches

13. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data, the Vendor shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.
14. We will record all data breaches regardless of their effect.
15. If the breach is likely to result in a high risk to data subject rights and freedoms, we will inform affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures that have been taken.

K. What are your individual rights in relation to your personal data?

1. The Processor is committed to take every reasonable step to:
    a. ensure that any personal data processed is up to date, accurate, adequate, relevant and not excessive, given the purpose for which it was collected;
    b. not process personal data obtained for one purpose for any other purpose, unless you agree to this or reasonably expect this;
    c. not release or sell your personal data to any third party for any purpose other than the processing of peer assessments.
2. You have several individual rights in relation to your personal data. You can require the Processor to:

a. provide access to your data;

b. rectify inaccurate data;

c. stop processing or erase data that is no longer necessary for the purposes of processing;

d. stop processing or erase data if your interests override the Processor's legitimate grounds for processing the data (where we rely on our legitimate interests as a reason for processing data);

e. stop processing data for a period if data is inaccurate or if there is a dispute about whether your interests override the Processor's legitimate grounds for processing the data.

3. To request that any of these steps be taken, please send the request to RobAnson@PeerAssessment.Com.

Right to access to personal data

4. Any data subject has a right to know what personal data have been collected concerning him or her, and to exercise that right easily and at reasonable intervals.

5. This right can be exercised by completing a subject access request (SAR) to obtain copies of records including personal information.

6. Subject Access Requests (SAR):

    a. Please submit a SAR in writing. To help us find the information, please note your name, institutional email, the class in which you used the System, the year and term in which you took the class, and if there are specific data or questions you seek to have addressed.

        i. To submit your request, either complete the SAR request form from your institution or send an email to RobAnson@peerassessment.com

    b. If you make a subject access request, the Vendor can provide the following information:

        i. the personal identification data of yours that we currently have stored;

        ii. for how long your personal data is stored (or how that period is decided);

        iii. any and all data calculations or visualizations which are available to Instructors to support grading or other evaluation decisions;

        iv. to whom your personal data is or may be disclosed;

        v. your rights of rectification or erasure of data, or to restrict or object to processing; and

        vi. your right to complain to the Information Commissioner if you think we have failed to comply with your data protection rights (if you attend an institution in a country following the GDPR).

7. For Students, our data minimization practices limit the amount of personal data we can retrieve. The following limits may apply:

    a. We can only retrieve a Student's historical personal data if we can associate it with their institutional email address. The history includes only the related personal data (academic location, assessment, response).

    b. The personal identifying data for Students is only stored while they are engaged in an active class loaded in the System. Once the class ends, we remove the personal identifying data elements

which, by design, are not recoverable.

8. For Instructors,
    a. Instructors' have registered accounts within the System that include their identifying data: name, institutional email, password (encrypted), and sometimes a phone number.
    b. Retrievable information includes only their identifying data and related usage data such as classes and terms taught, assessments created, and purchase information (if individually purchased). Assessment response data can be retrieved, but no Student identifying information will be available unless a class is currently active.

Student's right to rectify personal data inaccuracies

9. The Instructor is the primary Controller of Student information for a class. They load Student Identifiers into the System, determine what questions are asked, and create the procedures and expectations for conducting peer assessments in their class.
10. Students should take data change requests first to their instructor:
    a. The instructor can directly amend personal identifiers as well as the feedback entries made by a student about their teammates, or made by teammates about a student. Alternately, the instructor may ask the Processor to make specific changes for them.
    b. The Processor will readily assist the Instructor if they need help diagnosing or repairing data issues. However, to maintain the integrity of Student personal data, data changes should only be made by the Instructor, or by the Processor at the explicit request of the Instructor.

Instructor's right to rectify personal and related data inaccuracies or request erasure of personal data

11. The Instructor can directly update their personal identifying data (their account information) as needed, including Name, Email, Password.
12. If the Instructor needs to rectify inaccuracies in most of the related information they controlled in the System, they can:
    a. modify/delete class and assessment set up data (with some limitations);
    b. add/modify/remove Student identifying data from the class;
    c. update feedback entries made by students.
    d. request the Processor to assist them in making changes to their related information in the System, especially if they need help diagnosing or repairing data issues. However, to maintain the integrity of Instructor personal and related data, changes should only be made by the Instructor, or by the Processor at the explicit request of the Instructor.
13. If the Instructor seeks to terminate or suspend/restrict their personal data processing, they should send a written request to the Processor.
    a. To terminate an instructor, the Processor will pseudonymize the Instructor's email address identifying data and inactivate their password. If there are potentially active classes, these will be deleted (if they have not initiated assessments) or inactivated (if they have initiated assessments).

Student's right to request erasure or restriction of personal data

14. The GDPR requires that the Data Subject has the right to request, from the Controller, "...erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing."
15. Students should make such requests to their Instructor or the Institution's Governance Unit.
16. Should a Student request that their Student personal data be erased, or its processing suspended/restricted there are some limits and considerations:
    a. If the Student dropped the class:
        i. the Instructor should immediately remove the student from that class in the System.
        ii. this action will cause the System to remove the Student's association with that class and remove their identifying data (unless they are still loaded in some other active class.)
    b. If the Student remained in the class but was no longer working in a team:
        i. the Instructor should immediately remove the student from that class in the System if the Student requests that their data be removed.
        ii. this action will cause the System to remove the Student's association with that class and remove their identifying data (unless they are still loaded in some other active class.)
    c. If the Student remained in the class and was actively working in a team:
        i. removing one active team member from the System would impede peer assessments for the entire team. For this reason, the Vendor recommends that the instructor remove the entire team from the System and conduct their assessment on paper.
        ii. this action will cause the System to remove all of those Students' associations with that class and remove their identifying data (unless they are still loaded in some other active class.)