Pearson Data Protection and Security

Operative provisions:

1. Definitions

1.1 In this Data Protection and Security Schedule the following expressions have the following meanings:

“Agreement” means the provisions, exhibits, documents, and schedules of the Master Agreement (including but not limited to this DPSS)

"**Authorised Person**" means any person the Supplier authorises to process Pearson Data, which may include the Supplier's staff, agents and subcontractors;

"**Confidential Information**" only as used within this Schedule, is defined as:

(a) the existence and terms of this Agreement;

(b) all information disclosed to the relevant Party by or on behalf of the other Party in connection with the Agreement and which relates to the provisions of the Agreement, the negotiations relating to the Agreement or the subject matter of the Agreement;

(c) know-how, secret processes and inventions disclosed to the relevant party by or on behalf of the other party in connection with the Agreement;

(d) all other information disclosed to the relevant Party by or on behalf of the other Party (whether before, on or after the date of the Agreement) which is marked as or has been otherwise indicated to be confidential or which derives value to a Party from being confidential or which would be regarded as confidential by a reasonable business person;

“**Data Protection and Security Schedule (DPSS)**” means this Schedule;

"**Data Protection Laws**" means all applicable laws and regulations relating to the processing of personal data including, where applicable, the guidance and codes of practice issued by a regulator including implementing and supplemental legislation and the equivalent of any of the foregoing in any relevant jurisdiction; and including FERPA and HIPAA, where relevant, as defined below.

“FERPA”means the Family Educational Rights and Privacy Act codified in 20 U.S.C. § 1232g; 34 CFR Part 99) of U.S. Federal law and protects the privacy of student education records

“**HIPAA**” means the US Health Insurance Portability and Accountability Act of 1996;

“**PCI DSS**” means the Payment Card Industry Data Security Standard, as updated and maintained by the PCI Security Standards Council from time to time;

“**Pearson Data**” means Pearson’s Confidential Information, including Financial Data, Pearson Materials and Pearson Personal Information;

“**Pearson Materials**” means all text, images, literary and artistic works, photographic works, films, animations, videos, software, databases, instructions, documents, layout, design, trademarks and logos or similar materials which may be supplied by or on behalf of Pearson to the Supplier or be created by Supplier or on behalf of Supplier;

"**Pearson Personal Information**" means personal data processed by the Supplier as a processor or sub-processor for and on behalf of Pearson or its customers;

"**personal data**" means personal data, personal information, personally identifiable information or covered information related to an identifiable individual as applicable and defined under applicable Data Protection Laws;

"**controller**" has the meaning given to it under applicable Data Protection Laws, provided, however, that to the extent the applicable Data Protection Laws do not provide such definition or meaning, “controller” means and refers to the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

"**process**" has the meaning given to it under applicable Data Protection Laws, and "**processing**" and "**processed**" shall have the corresponding meaning; provided, however, that to the extent the applicable Data Protection Laws do not provide such definition or meaning, “process,” “processing” and “processed” mean and refer to any operation or set of operations performed on personal data, whether or not by automated means, including, without limitation, collection, recording, organisation, structuring, storage, adaptation, alteration, accessing, retrieval, consultation, use, disclosure by transmission, dissemination, distribution or making available by other means, alignment, combination, restriction, erasure, deletion or destruction;

"**processor**" has the meaning given to it under applicable Data Protection Laws, provided, however, that to the extent the applicable Data Protection Laws do not provide such definition and meaning, “processor” means and refers to a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

"**Security Incident**" means the loss of, or attempted or successful unauthorised access, use, disclosure, modification, or destruction of, any Pearson Data, other Pearson materials, or any information system that hosts or otherwise processes Pearson Data.

2. Scope and conflicts

2.1 The Parties acknowledge and agree that, for the purposes of the Agreement:

(a) Pearson is, or shall be regarded as, a controller of Pearson Personal Information and the Supplier is, or shall be regarded as, a processor of Pearson Personal Information; or

(b) Pearson is, or shall be regarded as, a processor of Pearson Personal Information (acting on behalf of its customers) and the Supplier is, or shall be regarded as, a sub-processor of Pearson Personal Information.

2.2 To the extent that any term of this DPSS conflicts with the terms of the rest of the Agreement then the terms of this DPSS shall prevail.

3. Processing instructions

3.1 The Supplier shall comply with all applicable laws and only process Pearson Personal Information in accordance with Pearson’s documented instructions (as set out in the Agreement as amended from time to time) except where otherwise required by any Data Protection Laws applicable to the relevant Pearson Personal Information.

3.2 In no event shall the Supplier process Pearson Data for its own purposes or the purposes of any third party.

4. Confidentiality of processing

4.1 Subject to any provision in this Agreement to the contrary Supplier shall treat all Pearson Data as strictly confidential and shall ensure that access and/or retrieval and other processing of Pearson Data is restricted to Authorized Persons only who have a legitimate and necessary reason to access, retrieve or otherwise process Pearson Data for purposes of performing the relevant Supply Agreement.

4.2 The Supplier shall ensure that all Authorised Persons are and shall continue to be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to process Pearson Data who is not under such a duty of confidentiality; and

4.3 The restrictions contained in this clause shall continue to apply after the termination of this Agreement (however arising) without limit in time.

5. Data Subject rights

5.1 The Supplier shall provide all reasonable and timely assistance (including by appropriate technical and organisational measures) to Pearson (at its own expense) to enable Pearson or, if applicable, a controller for whom Pearson is a processor, to respond to:

(a) any request relating to Pearson Personal Information from a data subject to exercise any of its rights under any Data Protection Laws (including its rights of access, correction, objection, erasure and data portability, as applicable);

(b) any request relating to Pearson Personal Information from a controller for access, correction, erasure, deletion and data portability, where Pearson is a processor of the Pearson Personal Information for such controller; and

(c) any other correspondence, enquiry or complaint received from a data subject, controller, regulator or other third party in connection with the processing of Pearson Data.

5.2 In the event that any such request, correspondence, enquiry or complaint is made directly to the Supplier, the Supplier shall promptly inform Pearson and provide full details of the request.

5.3 The Supplier shall not disclose any Pearson Data in response to a request for access or disclosure from any third party without Pearson's prior written consent, save where compelled to do so in accordance with applicable law.

6. Data protection impact assessments

If the Supplier believes or becomes aware that its processing of any Pearson Personal Information is likely to result in a high risk to the data protection rights and freedoms of data subjects, the Supplier shall promptly inform Pearson. In this circumstance and upon any other request by Pearson, the Supplier shall provide Pearson with all such reasonable and timely assistance as Pearson may require in order for Pearson to (or for Pearson to assist its customers to) conduct a data protection impact assessment and, if necessary, consult with its relevant data protection authority.

7. Records

The Supplier shall maintain records regarding the Supplier's processing of Pearson Personal Information, including data flow diagrams and the Supplier's processes for handling Security Incidents, for a period of two years following the completion of the Supplier's processing activities.

8. Security

8.1 The Supplier shall put in place and maintain a comprehensive information security program reasonably appropriate for the Pearson Data, which shall include implementing and maintaining all appropriate technical, security and organisational measures to protect Pearson Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access and against all other unlawful forms of processing.

8.2 The technical, security and organisational measures referred to under paragraph 8.1 shall at minimum meet the security requirements set out in Exhibit 2 to this DPSS.

8.3 Where the Supplier processes, transmits, and/or stores cardholder data and/or sensitive authentication data (as defined in PCI DSS) in the performance of services provided to Pearson, the Supplier shall comply with the provisions set out in Exhibit 3.

8.4 Where the Supplier accesses, stores or otherwise processes personal health information subject to HIPAA in the performance of its services provided to Pearson, the Supplier shall ensure that it executes and complies with a HIPAA Business Associate Agreement in the form set out in Exhibit 4.

9. Security Incidents

9.1 The Supplier shall notify Pearson immediately, and in any event no later than 24 hours after becoming aware (or after the Supplier should have reasonably become aware) of any Security Incident or any other breach of the Agreement. All such notifications should be made to the Pearson Security Operations Center (email: soc@pearson.com) in addition to any Pearson representative the Supplier regularly liaises with.

9.2 Upon becoming aware of the Security Incident, the Supplier shall:

(a) Promptly provide a summary report of the Security Incident with sufficient detail to enable Pearson to comply with any and all laws and regulations, which shall include at least the following information (if known):

(1) the date, time, and description (including root cause) of the Security Incident;

(2) how the Security Incident was detected;

(3) the systems and data affected;

(4) whether the Security Incident included Pearson Personal Information;

(5) a list of all Pearson Data disclosed as a result of the Security Incident;

(6) any corrective action taken; and

(7) any additional planned or required corrective actions.

(b) Immediately take all such measures and actions as are necessary to remedy or mitigate the effects of Security Incidents and shall keep Pearson up-to-date about all developments in connection with Security Incidents.

(c) For the duration of the Security Incident and corresponding investigation of the Security Incident and any notifications of the Security Incident Pearson makes to a regulator, provide full and timely cooperation, assistance, documents and information to Pearson including, but not limited to, any audit assessments or analyses related to the Security Incident and any other commercially reasonable actions reasonably requested by Pearson:

9.3 Upon request of Pearson, Supplier, within five (5) days of the closure of the Security Incident, shall provide Pearson will a written report describing the Security Incident, the actions taken by the Supplier during its response and the Supplier's plans for future actions to prevent a similar incident from occurring.

9.4 If requested by Pearson, in the event of a Security Incident which results in, or requires, notification to data subjects affected by the Security Incident as a result of Supplier's processing of any Pearson Personal Information, the Supplier shall prepare and provide notification of the Security Incident in a form approved by Pearson, and paid for by the Supplier, to each data subject. .

9.5 The Supplier shall not make any public statements about, or notify a regulator of, a Security Incident without Pearson's prior written consent.

10. Sub-processors

10.1 The Supplier shall not provide access to, disclose, or engage any subcontractors, or other third party, to process Pearson Data unless:

(a) Pearson provides express, prior, written authorisation, and

(b) Supplier imposes terms on the subcontractor, or other third party, which are no less onerous than those imposed upon the Supplier under the Agreement and, upon request of Pearson, will provide copies of the signed agreements with Suppliers subcontractors pursuant to this provision 10, and

(c) Supplier provides Pearson at least 60 days' prior notice of the addition or modification of any subcontractor listed in the attached Exhibit 1 (including details of the processing it performs or will perform in relation to Pearson Data) and

(d) Pearson has not objected to the addition of sub-contractor (and, in the event that Pearson objects to the addition of such sub-contractor then either the Supplier shall not appoint the subcontractor or Pearson may elect to suspend or terminate the Agreement without penalty);

10.2 Notwithstanding clause 10.1, as of the date of the Agreement:

(a) Pearson consents to the subcontractors listed in the attached Exhibit 1 and

(b) Supplier warrants that it has imposed data protection terms on the listed subcontractors in accordance with 10.1 (b) and;

10.3 The Supplier shall remain fully liable for any breach of the Agreement that is caused by an act, error or omission of any of its subcontractors who are processing Pearson Data.

11. Audit and records retention

11.1 If requested by Pearson and no more than once annually, the Supplier will make available to Pearson all information necessary to demonstrate compliance with the obligations set forth in the Agreement and allow for and contribute to audits, including inspections, conducted by Pearson or another auditor mandated by Pearson. The details of such audit will include, but are not limited to, the details contained in Section 6 of Exhibit 2

11.2 The Supplier shall maintain accurate and detailed records relating to its compliance with this DPSS for a period of two (2) years after the termination or expiration of the Agreement in a format that will permit assessment or audit..

12. International data transfers

The supplier shall not process Pearson Data across international borders unless it: (a) first obtains Pearson's prior written consent and; (b) takes all such measures as are necessary to ensure that any processing of such Pearson Data is carried out in accordance with applicable legislation and any applicable or required transfer mechanisms.

13. Indemnity

The Supplier shall indemnify and defend Pearson from and against any and all claims, actions, loss, cost, harm, expense (including court costs and reasonable legal fees), liabilities or damage ("Damage") suffered or incurred by Pearson or made by any third party as a result of or in connection with the failure of the Supplier or any Supplier subcontractor to comply with any of the Supplier's obligations under this Data Protection and Security Schedule, provided that Pearson:

(a) gives the Supplier prompt notice of any circumstances of which it is aware that give rise to an indemnity claim under this paragraph; and

(b) takes reasonable steps and actions to mitigate any ongoing Damage it may suffer as a consequence of the Supplier's failure to comply with any of its obligations under this DPSS.

14. Effects of termination

14.1 Upon termination of the Agreement, the Supplier shall immediately cease processing the Pearson Data.

14.2 Subject to paragraph 16.3, upon termination of the Agreement the Supplier shall (at Pearson's election) destroy or return to Pearson all Pearson Data (including all copies of Pearson Data) in its possession or control (including any Pearson Data subcontracted to a third party for processing).

14.3 Paragraph 16.2 shall not apply to the extent that the Supplier is required by any applicable law to retain some or all of the Pearson Data, in which case Supplier shall isolate and protect such Pearson Data from any further processing except to the extent required by such law.

Pearson Global Security Compliance Requirements for Suppliers and Partners

Part A: Introduction

1. **Overview**. This security exhibit (the "**Exhibit**") sets out Pearson's minimum security requirements (the "**Requirements**").

2. **Definitions**. Words and expressions not defined elsewhere in this Agreement shall have the meanings set out in Annex A to this Exhibit.

3. **Relationship with rest of Agreement**. The provisions in this Exhibit are without prejudice to the provisions in the remainder of this Agreement. However, if any term in this Exhibit directly conflicts with a term of this Agreement, then the term of this Agreement shall prevail.

4. **Updates**. Pearson reserves the right to update or otherwise modify its requirements in this Exhibit from time to time. Upon notice by Pearson to the Supplier that the Requirements have been updated or modified, the revised version of the Requirements shall apply.

Part B: General Supplier Obligations

5. The Supplier shall implement and maintain a policy that prohibits the use of any devices that are not administered and/or managed by Supplier, Supplier's approved sub-processors or Pearson to access and/or store Pearson Data.

6. Audit

6.1 Supplier shall allow for, and contribute to, audits. Specifically, Supplier shall:

(a) No more than once annually, the Supplier shall complete and return to Pearson, within 30 days of receipt, a Pearson audit survey unless the Supplier can provide an independently certified IEC/ISO27001 or SOC2 compliance report and SOC1/SSAE18 report where applicable.

(b) Any findings made as a result of the audit survey completed by Supplier under this clause 11 will be addressed in a mutually agreed upon remediation plan and the Supplier shall complete and comply with such remediation plan within a mutually agreeable timeframe set forth therein. Failure to correct or remediate findings shall be considered a material breach of this Agreement and of any Supply Agreement.

(c) If Pearson elects to exercise any of its audit and inspection rights it holds in relation to the records and practices of such sub-processors, the Supplier shall cooperate with Pearson in procuring the compliance of its sub-processors, including procuring that its sub-processors complete a Pearson audit survey.

(d) Within thirty (30) days of Pearson's receipt of an assessment or audit report, the Supplier shall provide Pearson with a written report outlining the corrective actions that the Supplier has implemented or proposes to implement with the schedule and status of each corrective action.

Part C: Information Security Requirements

7. **General Security Requirements**. The Supplier shall:

7.1 Be compliant with applicable government legislation and industry mandated information security standards (examples of such standards include, but are not limited to, ISO/IEC 27001, the Payment Card Industry-Data Security Standards (PCI-DSS), Electronic Data Interchange (EDI) standards, and the information security requirements documented within laws, such as the Health Insurance Portability and Accountability Act - HIPAA.)

7.2 Establish and maintain a formal and comprehensive security program in accordance with Industry Best Practice with reasonable and appropriate administrative, organizational, technical, and physical safeguards, including those set out in this Part C (the "**Information Security Requirements**"), designed to ensure the confidentiality,

integrity, and availability of Pearson Data (including, without limitation, the privacy of Pearson Data) and to guard against Security Incidents. Such data safeguards will include, but are not limited to, the following:

(a) Supplier shall maintain an inventory of systems used by Supplier to store or process Pearson Data;

(b) Supplier shall have a media and non-volatile storage sanitization and destruction policy and procedure, which:

(i) meets at a minimum, NIST SP 800-88 Purge and Destruction requirements; and

(ii) includes the issuance of a certificate of destruction or sanitization to Pearson that Pearson Data is properly wiped or destroyed,

so as not to allow for any type of data recovery at any time during or at the end of the term of this Agreement or as requested by Pearson;

(c) Any hard copy materials containing Pearson Data or related application support shall be secured in locked containers when not in use,and destroyed by secure shredding at any time during or at the end of the term of this Agreement or as requested by Pearson. Certificate(s) of Destruction may be requested by Pearson;

(d) Isolate Pearson's applications and Pearson Data from any other customer's or Supplier's own applications and information by using assured separation servers

(e) Have documented procedures for the secure backup and recovery of Pearson Data, which shall include, at a minimum, Strong Encryption, secure procedures for the transport, storage, and disposal of the backup copies of Pearson Data, with documented chain of custody.

(f) Use Strong Encryption to protect Personal Information when transmitted and stored.

8. **Personnel or Staff Security**

(a) The Supplier shall, where legally permissible, complete a comprehensive background investigation on all employees before providing access to Pearson Data including verification of the identity, address, employment history/eligibility, professional qualifications of any member of Supplier's team and performing additional checks such as drug screening or criminal records (where available);

(b) The Supplier shall have a formal policy on conditions and timelines for access to Pearson or supplier systems to be given to individuals joining, changed for individuals moving to different roles, and removed for those individuals leaving for any reason.

(c) The Supplier shall ensure all Authorized Persons have relevant, reasonable and necessary training and experience.

(d) The Supplier shall ensure that all Authorised Persons who handle Pearson Data are informed of the confidential nature of Pearson Data and have undertaken appropriate training regarding their obligations in connection with their handling of that Data including applicable laws and regulations, potential security or breach reporting obligations and acceptable use of and proper procedures for storing and transmitting Pearson Data. Supplier shall maintain records of this training and will make those records available to Pearson upon request

9. System Security. The Supplier shall:

9.1 Where applicable, the supplier complies with their Cloud Hosting Provider's shared security model and the best practises described by the Cloud Security Alliance, Cloud Control Matrix.

9.2 Protect Pearson Data by implementing information resources such that they are logically segmented based on the similarity of purpose and ensure that each segment is separated and protected with devices and services

(i.e. Web and Network Security Gateways, Firewalls, etc) configured and hardened to act as security enforcing points.

9.3 In all cases, use Strong Encryption (e.g. FIPS 197) to protect Pearson Data in transit when transmitted or at rest.

9.4 Where applicable, deploy network or cloud protective controls capable of detecting and blocking malicious traffic entering and leaving the Supplier's Information Resources.

9.5 Only remove Pearson Data from outside of their direct control if authorized in writing by Pearson. If so authorized (e.g., in connection with offsite storage of data backups), such Pearson Data may only be transported on devices configured with full disk encryption to protect the data from loss or theft.

9.6 Not store Pearson Data on removable media (e.g., USB flash drives, thumb drives, memory sticks, tapes, CDs, or external hard drives) except: (a) for backup, business continuity, disaster recovery, and data interchange purposes as allowed and required under this Agreement, and (b) in all cases using Strong Encryption.

9.7 Ensure that all of the Supplier's Information Resources are and remain 'hardened' in accordance with the center for internet security hardening benchmark (https://www.cisecurity.org/) and/or vendor supplied security administrative guide.

10. **Security Gateways**. The Supplier shall:

10.1 Require Strong Authentication for administrative and/or management access to Security Gateways, including any access for the purpose of reviewing log files.

10.2 Have and use documented controls, policies, processes and procedures to ensure that unauthorized users do not have administrative and/or management access to Security Gateways, and that user authorization levels to administer and manage Security Gateways are appropriate.

10.3 At least once every six (6) months, ensure that Security Gateway configurations are hardened by selecting a sample of Security Gateways and verifying that each default rule set and set of configuration parameters are implemented.

10.4 Use monitoring tools to validate that all aspects of Security Gateways (e.g., hardware, firmware, and software) are continuously operational.

10.5 Configure and implement all Security Gateways such that all non-operational Security Gateways shall deny all access.

10.6 Configure real-time alerting for changes to the Security Gateway configuration and/or rule base.

11. **Connectivity Requirements**. In the event that Supplier has, or will be provided, connectivity to Pearson's or Pearson's customers' Nonpublic Information Resources, it shall:

11.1 Use only the mutually agreed upon facilities and connection methodologies to interconnect Pearson's and Pearson's customers' Nonpublic Information Resources with Supplier's Information Resources.

11.2 NOT establish interconnection to Pearson's and Pearson's customers' Nonpublic Information Resources without the prior written consent of Pearson.

11.3 Provide Pearson access to any applicable Supplier facilities during normal business hours for the maintenance and support of any equipment (e.g., router) provided by Pearson for connectivity to Pearson's and Pearson's customers' Nonpublic Information Resources.

11.4 Use any equipment provided by Pearson for connectivity to Pearson's and Pearson's customers' Nonpublic Information Resources only for the furnishing of those services or functions explicitly authorized by Pearson.

11.5 If the agreed upon connectivity methodology requires that Supplier implement a Security Gateway, maintain logs of all sessions using such Security Gateway. These session logs must include sufficiently detailed information to

identify the end user or application, origination IP address, destination IP address, ports/service protocols used and duration of access. These session logs must be retained for a minimum of twelve (12) months.

11.6 Permit Pearson to gather information relating to access, including Supplier's access, to Pearson's and Pearson's customers' Nonpublic Information Resources. This information may be collected, retained and analyzed by Pearson to identify potential security risks without further notice. This information may include trace files, statistics, network addresses, and the actual data or screens accessed or transferred.

11.7 Shall permit Pearson to immediately suspend or terminate any interconnection to Pearson and Pearson's customers' Nonpublic Information Resources if Pearson, in its sole discretion, believes there has been a Security Incident or unauthorized access to or misuse of Pearson Data or Pearson Information Resources.

12. **Identification and Authentication**.

12.1 In relation to access to Pearson Data, either in electronic or hard copy, by the Supplier's team, the Supplier shall:

(a) Require Strong Authentication (i.e. Multi-factor authentication) for any remote access use of non-public Information Resources

(b) Ensure that access to systems that process Pearson Data is enforced through a centralized identity provider that conforms to industry best practise.

(c) Use a secure method for the conveyance of authentication credentials (i.e. passwords) and authentication mechanisms (i.e. tokens or smart cards)

(d) Where appropriate adopt a risk-based authentication mechanism such that authentication methods are tiered and proportionate to the sensitivity of the Pearson Data to be accessed (i.e. the use of stronger form of authentication for accessing Pearson Personal Information)

(e) Have and use a documented User ID lifecycle management process including procedures for approved account creation, account removal immediately on termination or within 24 hours on role change, and account modification (i.e. changes to privileges, span of access, functions/roles) for all Information Resources and across all environments (e.g., production, test, development, etc.). Such process shall include review of access privileges and account validity to be performed at least quarterly.

13. **Software and Data Integrity**. The Supplier shall:

13.1 Ensure all its computer, network and storage resources are configured to utilize security capabilities that detect, quarantine and prevent against malicious code execution.

13.2 If the Supplier is developing an application for Pearson, ensure that any solution it uses to process Pearson Data is free of common web application security vulnerabilities as defined by, but not limited to, the OWASP top 10.

13.3 Separate non-production Information Resources from production Information Resources using distinctive computer, network, and storage resources.

13.4 Use only masked data in development and test environments. If this is not possible, the Supplier must obtain Pearson's written approval to use non de-identified Pearson Data and the Supplier warrants and undertakes that such environments have access controls as rigorous as those used in production.

13.5 Have a documented change control process including security impact review and back-out procedures for all production environments.

13.6 For applications which utilize a database that allows modifications to Pearson Data, the Supplier shall have database transaction logging features enabled and retain database transaction logs for a minimum of twelve (12) months.

13.7 Review such software to find and remediate all security vulnerabilities (static, dynamic and dependency code analysis) prior to initial implementation and upon any modifications and updates for all software developed under an agreement with the Supplier.

13.8 Perform quality assurance testing (using CREST and/or CHECK accredited security assessor) for the security components (e.g., testing of identification, authentication, authorization, confidentiality, integrity, availability, non-repudiation functions), as well as any other activity designed to validate the security architecture, during initial implementation and upon any modifications and updates.

14. Vulnerability Scanning & Penetration Testing. During the term of this Agreement or while Pearson Data is processed by Supplier (whichever is later), the Supplier shall:

14.1 Use industry standard tools and manual techniques to assess the security of solution(s) provided by the Supplier and used in support of Pearson employees, Pearson suppliers, and/or Pearson customers.

14.2 Perform at least quarterly, and immediately following all significant changes and upgrades, a vulnerability scan externally and internally facing Information Resources, including networks, servers, applications and databases, with applicable industry-standard security vulnerability scanning software to uncover security vulnerabilities, ensure that such Information Resources are properly hardened.

14.3 Test, at least quarterly, to identify any unauthorized wireless networks.

14.4 Upon request, the Supplier will provide Pearson a copy of the Vulnerability Scanning results, which shall be treated as Supplier Confidential Information unless disclosure is otherwise required by applicable law.

14.5 Have a third-party complete penetration testing at least annually and provide the results to Pearson on request. In the event vulnerability findings are identified as a result of this testing, the Supplier shall provide, in a timely manner, sufficient technical personnel and support to fix the issues identified and to continue conducting further ethical hacks until Pearson is assured that the identified incidents and their underlying causes have been cured.

15. **Logging**. The Supplier shall:

15.1 Log privileged accounts on all devices and applications.

15.2 Log record access (read), write, change, logon attempts, failed access attempts, changes to access controls lists, identifiers, or group/role privileges, updates to security software or the functionality of software and applications, and execution of any program that can bypass access controls.

15.3 Implement a real-time logging server and restrict access to security logs to authorized individuals, and protect security logs from unauthorized modification and a centralized means of monitoring security logs. All security and security-related audit logs for anomalies shall be reviewed no less than weekly, and resolve all logged security problems in a timely manner.

15.4 Retain all security and server logs for a period of one year (with 90 days available online) or as required to comply with regulatory requirements, whichever is greater. The log will record all logical access attempts both valid and invalid. The log will include the name (ID), data and time of the login, records accessed, and activity performed. If possible, the log will also have an entry for log-out.

16. **Physical Security**. The Supplier shall:

16.1 Ensure that all systems used to process and store Pearson Data will be in secure, monitored and access-controlled premises;

16.2 Locate all Information Resources in secure hosted facilities with access limited and restricted to authorized individuals only;

16.3 Locate all Information Resources in geographies that provide an adequate legal framework to ensure compliance with the terms and conditions of this Agreement;

16.4 Monitor and record, for audit purposes, access to the physical facilities hosting Information Resources intended for use by multiple users, including the name of the employee, time and date of entry and exit, and where feasible, monitor the room by camera.

17. **Mobile and Portable Devices**. The Supplier shall:

17.1 Not use network aware Mobile and Portable Devices that are not laptop computers ("network aware devices") to access and/or store Pearson Data, without Pearson's express prior written approval.

17.2 Review, at least annually, the use of, and controls for, all Supplier-administered or -managed Mobile and Portable Devices to ensure that the Mobile and Portable Devices can meet the applicable Information Security Requirements.

18. **Wireless Networking**. If approved in writing by Pearson, when using radio frequency (RF) based wireless networking technologies to perform or support Services for Pearson, the Supplier shall ensure that all Pearson Data transmitted is protected by the use of appropriate encryption technologies sufficient to protect the confidentiality of Pearson Data.. The use of RF-based wireless headsets, keyboards, microphones, and pointing devices, such as mice, touch pads, and digital drawing tablets, is excluded from this requirement.

19. **Pearson Owned or Provided Devices**. The Supplier shall return all Pearson-owned or -provided devices (including personal systems, tokens and/or software) as soon as practicable, but in no event more than fifteen (15) days after the sooner of: (a) expiration or Termination of this Agreement; (b) Pearson's request for the return of such property; or (c) the date when the Supplier no longer needs such devices.

20. **Call Recording Data**. If the Supplier is processing Call Recording Data on behalf of Pearson, then this paragraph shall apply to the Supplier:

20.1 Software Requirements for Collecting Call Recording Data:

(a) Software used for processing Call Recording Data must provide individual, authenticated accounts with an access audit trail.

(b) Software used for processing Call Recording Data must have the capability to turn recordings on or off.

20.2 Enablement of Supplier's Call Recording Capabilities:

(a) The Supplier shall not enable, activate, nor make operational any call recording capabilities for Call Recording Data collected and processed on behalf of Pearson unless (1) requested by and (2) approved by Pearson in writing.

(b) The percentage of Call Recording Data recorded by the Supplier must comply with the percentage allowed in writing by Pearson. Specific permission must be obtained for 100% recording of Call Recording Data.

(c) If the Supplier intends to use Call Recording Data for the Supplier's internal training purposes, the Supplier shall use utilize technical mechanisms to redact all personal data and sensitive personal data from Call Recording Data.

20.3 Notice of Recording:

(a) Prior to recording Call Recording Data, the Supplier shall notify a party that the Supplier is about to record the conversation (a "**Recording Notice**").

(b) The Supplier shall ensure the Recording Notice:

(i) complies with all applicable laws and regulations.

(ii) includes the clear and specific purpose of the recording, such as for quality monitoring, workforce management, agent and customer service representative training, evaluation and verification, dispute resolution or accurate incident reconstruction.

(c) The Supplier shall implement a Recording Notice for both inbound recorded calls received by and outbound recorded calls made by Supplier.

20.4 Option Not to Record:

The Supplier's processes shall include the ability not to record inbound and outbound calls if so requested by the initiator of the call while still providing the requested service(s) to Pearson.

20.5 Use and Access of Call Recording Data:

(a) Use of the Call Recording Data must be consistent with the Recording Notice.

(b) Call Recording Data must only be accessed by authorized users with accounts on the call recording system.

(c) Call Recording Data must not be shared through email or stored using other electronic distribution methods such as file shares unless otherwise authorized in writing by Pearson.

20.6 Storage and Transmission of Call Recording Data:

(a) The Supplier shall protect filed or electronically stored Call Recording Data in accordance with this Agreement and applicable law.

(b) The Supplier shall encrypt sensitive personal data in storage and in transit.

20.7 Copies of Call Recording Data:

(a) The Supplier must have Pearson's written authorization prior to making any copy, archival copy, or reproduction of Call Recording Data Processed on behalf of Pearson.

(b) Copies, archival copies and reproductions of Call Recording Data are subject to the same access control and data protection requirements as the original Call Recording Data.

20.8 Call Recording Data Retention:

(a) The Supplier shall promptly delete Call Recording Data after the Supplier satisfies the specific purpose stated in the Recording Notice.

(b) The Supplier shall not retain Call Recording Data for no longer than the shorter of (i) the maximum period specified under applicable law; or (ii) sixty (60) calendar days after the original recording was made, unless otherwise authorized by Pearson in writing.

20.9 Call Recording Data:

The Supplier shall comply with all applicable laws when processing Call Recording Data including applicable laws concerning Recording Notices, consent, transfers of Call Recording Data outside country borders and restrictions on types of information that may be received.

Annex A

Definitions

"**Demilitarized Zone**" or "**DMZ**" shall mean a network or sub-network that sits between a trusted internal network, such as a corporate private Local Area Network (LAN), and an untrusted external network, such as the public Internet. A DMZ helps prevent outside users from gaining direct access to internal Information Resources.

"**Call Recording Data**" shall mean any data that is recorded and/or stored relating to Pearson employee and customer interaction voice calls including calls across transfers, holds, conference calls, inbound and outbound calls.

"**Industry Best Practice**" means processes and technology processes that form of practice reasonably expected of a leading supplier in the same or substantially similar sector seeking to comply with its regulatory and contractual responsibilities."

"**Information Resource(s)**" means systems, applications, networks, network elements, and other computing and information storage devices, including smart phones, tablets, and USB memory sticks.

"**Mobile and Portable Devices**" means mobile and/or portable computers, devices, media and systems capable of being easily carried, moved, transported or conveyed. Examples of such devices include laptop computers, tablets, USB hard drives, USB memory sticks, Personal Digital Assistants (PDAs), and wireless phones, such as smartphones.

"**Nonpublic Information Resources**" means those Information Resources to which access is restricted and cannot be gained without proper authorization and identification.

"**Security Gateway**" shall mean a set of control mechanisms between two or more networks having different trust levels which filter and log traffic passing, or attempting to pass, between networks, and the associated administrative and management servers. Examples of Security Gateways include firewalls, firewall management servers, hop boxes, session border controllers, proxy servers, and intrusion prevention devices.

"**Strong Authentication**" means the use of authentication mechanisms and authentication methodologies stronger than the passwords required under the Requirements. Examples of Strong Authentication mechanisms and methodologies include digital certificates, two-factor authentication, and one-time passwords.

"**Strong Encryption**" means the use of encryption technologies with minimum key lengths of 256-bit for symmetric encryption and 1024-bits for asymmetric encryption whose strength provides reasonable assurance that it will protect the encrypted information from unauthorized access and is adequate to protect the confidentiality and privacy of the encrypted information, and which incorporates a documented policy for the management of the encryption keys and associated processes adequate to protect the confidentiality and privacy of the keys and passwords used as inputs to the encryption algorithm.

PCI Compliance Exhibit

Whereas Pearson is required to adhere to the Payment Card Industry Data Security Standard (PCI DSS) promulgated by the PCI Security Standards Council; and

Whereas Supplier processes, transmits, and/or stores cardholder data in the performance of services provided to Pearson, and is therefore considered a "service provider" under Requirement 12.8 of the PCI DSS; and

Whereas Requirement 12.8.2 of the PCI DSS requires Pearson to maintain a written agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data that the service provider possesses; and

Whereas Requirement 12.8.4 of the PCI DSS requires Pearson to maintain a program to monitor the service provider's PCI DSS compliance status,

1. Supplier agrees that it is responsible for the security of cardholder data and sensitive authentication data (as defined in PCI DSS) that it possesses, including the functions relating to storing, processing, and transmitting of the cardholder data.

2. Supplier affirms that, as of the effective date of this Agreement, it has complied with all applicable requirements to be considered PCI DSS compliant, and has performed the necessary steps to validate its compliance with the PCI DSS.

3. Supplier agrees to supply to Pearson the current status of Supplier's PCI DSS compliance status, and evidence of its most recent validation of compliance, upon execution of this Agreement. Supplier must supply to Pearson a new status report and evidence of validation of compliance at least annually.

4. Supplier will immediately notify Pearson if it learns that it is no longer PCI DSS compliant and will immediately provide Pearson the steps being taken to remediate the non-compliance status. In no event should Supplier's notification to Pearson be later than seven (7) calendar days after Supplier learns it is no longer PCI DSS complaint.

5. Supplier acknowledges that any indemnification provided for under this Agreement applies to the failure of the Supplier to be and to remain PCI DSS compliant.

6. Supplier represents and warrants that for the life of this Agreement, the software and services used for processing transactions shall be compliant with standards established by the PCI Security Standards Council (https://www.pcisecuritystandards.org/index.shtml), as amended from time to time. Supplier agrees to indemnify and hold Pearson, its officers, employees, and agents, harmless for, from and against any and all claims, causes of action, suits, judgments, assessments, costs (including reasonable attorneys' fees) and expenses arising out of or relating to any loss of Pearson customer credit card or personally identifiable information managed, retained or maintained by Supplier, including but not limited to fraudulent or unapproved use of such credit card or identity information.